ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Σάμος, Φεβρουάριος 2023

Κυβερνοασφάλεια και καταγραφή νέων μορφών απειλών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΜΜΑΝΟΥΗΛ ΚΑΡΡΑΣ

ICSD09053

Επιβλέπουσα Καθηγήτρια

Καρύδα Μαρία

Αναπληρώτρια Καθηγήτρια

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Κυβερνοασφάλεια και καταγραφή σύγχρονων και νέων μορφών απειλών

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΕΜΜΑΝΟΥΗΛ ΚΑΡΡΑΣ

Επιβλέπων Καθηγητής

Καρύδα Μαρία

Αναπληρωτής Καθηγήτρια

Εγκρίθηκε από την τριμελή Εξεταστική Επιτροπή

Μ. Καρύδα	Σ. Κοκολάκης	Κ. Μαλιάτσος
Καθηγητής 1	Καθηγητής 2	Καθηγητής 3

Σάμος, Φεβρουάριος 2023

Εμμανουήλ Καρράς

Φοιτητής Μηχανικός Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Αφιερώνεται στην οικογένειά μου

Περίληψη

Η αυξανόμενη εξάρτηση των οργανισμών από την ψηφιακή τεχνολογία έχει αυξήσει την ανάγκη για πολιτικές και μέτρα κυβερνοασφάλειας για την προστασία ευαίσθητων δεδομένων και λειτουργιών. Αυτή η διατριβή εξετάζει τις απειλές για την κυβερνοασφάλεια που αντιμετωπίζουν οι οργανισμοί και τις καταστροφικές συνέπειες που μπορεί να προκύψουν εάν δεν ληφθούν τα απαραίτητα μέτρα. Παρέχει επίσης μια λεπτομερή ανάλυση των μέτρων που μπορούν να ληφθούν για την προστασία οργανισμών, επιχειρήσεων και ατόμων από κυβερνοεπιθέσεις, ανάλογα με τον τύπο της επίθεσης. Επιπλέον, η παρούσα διατριβή αναλύει σε βάθος τις βασικές πολιτικές κυβερνοασφάλειας που πρέπει να ακολουθήσει κάθε οργανισμός και άτομο για να εργαστεί σε ένα ασφαλές περιβάλλον. Μέσα από την έρευνα, διαπιστώθηκε ότι δεν είναι ιδιαίτερα δύσκολο να διασφαλιστεί ένα ασφαλές εργασιακό περιβάλλον από τεχνική άποψη. Ωστόσο, η δυσκολία και η αποτελεσματικότητα των πολιτικών κυβερνοασφάλειας εξαρτώνται από τη συνεργασία πολλών τμημάτων. Επιπλέον, η εφαρμογή μιας πολιτικής κυβερνοασφάλειας δεν μπορεί να εγγυηθεί ότι θα ακολουθείται αυστηρά από όλο το προσωπικό. Συμπερασματικά, η παρούσα διατριβή υπογραμμίζει τη σημασία των πολιτικών κυβερνοασφάλειας στο σύγχρονο ψηφιακό περιβάλλον και υπογραμμίζει τη σημασία της λήψης των απαραίτητων μέτρων για την προστασία οργανισμών, επιχειρήσεων και ατόμων από κυβερνοεπιθέσεις.

Abstract

The increasing dependence of organizations on digital technology has raised the need for cybersecurity policies and measures to protect sensitive data and operations. This thesis examines the threats to cybersecurity that organizations face and the devastating consequences that can occur, if necessary, actions are not taken. It also provides a detailed analysis of the measures that can be taken to protect organizations, businesses, and individuals from cyber-attacks, depending on the type of attack. Moreover, this thesis analyzes in-depth the essential cybersecurity policies that every organization and individual must follow to work in a secure environment. Through the research, it was found that it is not particularly challenging to ensure a secure working environment from a technical perspective. However, the difficulty and effectiveness of cybersecurity policies depend on the cooperation of many departments. Furthermore, the application of a cybersecurity policy cannot guarantee that it will be strictly followed by all personnel. In conclusion, this thesis emphasizes the significance of cybersecurity policies in the modern digital environment, and it highlights the importance of taking the necessary measures to protect organizations, businesses, and individuals from cyber-attacks.

Περιεχόμενα

Περιεχόμενα Εικόνων

ΚΕΦΑΛΑΙΟ 1. ΕΙΣΑΓΩΓΗ

1.1 Θεωρητικό Υπόβαθρο

Ο σημερινός κόσμος είναι περισσότερο από ποτέ εξαρτημένος και συνυφασμένος με τη χρήση της τεχνολογίας, το οποίο είναι αποτέλεσμα της έντονης εξέλιξης και εισαγωγής της τεχνολογίας τόσο στον κόσμο των επιχειρήσεων όσο και στην προσωπική ζωή των ανθρώπων. Ως εκ τούτου, αποτέλεσμα της κυριαρχίας των τεχνολογιών στην ανθρώπινη καθημερινότητα είναι η ανάδυση και ανάπτυξη τεχνολογιών με θετικό αντίκτυπο στην ζωή όλων. Παρόλα αυτά, δεν λείπουν από την άλλη οι κακόβουλες οντότητες/λογισμικά που στόχο έχουν να επιβουλευτούν την διείσδυση αυτή της τεχνολογίας στην καθημερινότητα των ανθρώπων, γνωστά με τον όρο κυβερνοεπιθέσεις.

Ως κυβερνοεπίθεση αναφέρεται κάθε κακόβουλη δραστηριότητα που έχει ως στόχο τη συλλογή, διαταραχή, άρνηση, υποβάθμιση ή καταστροφή πόρων ενός πληροφοριακού συστήματος ή ακόμη και της ίδια της πληροφορίας. Μοναδικός σκοπός αυτής της επιθετικής δραστηριότητας είναι η αθέμιτη πρόσβαση σε δεδομένα και η διατάραξη της ομαλής λειτουργίας του συστήματος (Zhuang et al., 2015). Οι στόχοι τέτοιου είδους κυβερνοεγκλημάτων είναι πάρα πολλοί και πολλές φορές ιδιαίτερα σημαντικοί και ευαίσθητοι, ιδιαίτερα στον επιχειρηματικό κόσμο. Ενδεικτικά αναφέρονται η επίθεση και υποκλοπή σημαντικών στρατηγικών πόρων της επιχείρησης, όπως για παράδειγμα βιομηχανικά συστήματα τα οποία ελέγχουν δίκτυα ηλεκτροδότησης, ύδρευσης ή άλλων σημαντικών υποδομών (Bendovschi, 2015). Οι επιπτώσεις της στις επιχειρήσεις οι οποίες μπορεί να πέσουν θύματα κυβερνοεπιθέσεων, είναι πολλές φορές μη αναστρέψιμες και διακρίνονται σε (Bendovschi, 2015· McGavran, 2009):

- **Οικονομικές:** Κλοπή πνευματικής ιδιοκτησίας, κλοπή εταιρικών πληροφοριών, κόστος φθοράς ζημιών ενός συστήματος.
- **Φήμη:** Απώλεια της εμπιστοσύνης των καταναλωτών, απώλεια του υπάρχοντος πελατολόγιου καθώς και φυγή δυνητικών μελλοντικών πελατών.
- **Νομικές**: Δημιουργία καταστάσεων που επισύρουν αγωγές, πρόστιμα και κυρώσεις όπως για παράδειγμα λόγω παραβιάσεων της νομοθεσίας GDPR.

Λειτουργικές: Διακοπή στη λειτουργία σημαντικών πληροφοριακών συστημάτων που μπορεί να προκαλέσει διαταραχή στον τρόπο λειτουργίας μιας επιχείρησης.

Από την άλλη, σε ατομικό επίπεδο, πολλές φορές οι κακόβουλες ενέργειες, όπως η διαρροή προσωπικών δεδομένων, μπορεί να προκαλέσουν κλοπή της προσωπικής ταυτότητας των πολιτών. Για παράδειγμα, πολλές φορές υποκλέπτονται ευαίσθητα προσωπικά δεδομένα, όπως αριθμοί κοινωνικής ασφάλισης, οικονομικά στοιχεία κ.λπ., τα οποία αποθηκεύονται σε υπηρεσίες cloud και συνήθως μπορεί να υποκλέπτονται ακόμα και από προσωπικούς λογαριασμούς στα κοινωνικά δίκτυα. Άλλες εφαρμογές υποκλοπής αναφέρονται επίσης σε ηλεκτρονικές υπηρεσίες όπως το DropBox και το Google Drive (Von Solms & Van Niekerk, 2013) (Von Solms & Van Niekerk, 2013). Για το σκοπό αυτό, πολλές κυβερνήσεις σε όλο τον κόσμο οδηγούνται σε νομοθετικές ενέργειες οι οποίες σκοπό έχουν την προστασία των προσωπικών δεδομένων, με χαρακτηριστικό παράδειγμα το GDPR της Ευρωπαϊκής Ένωσης (Zerlang, 2017).

Πρωταρχικός στόχος όλων των νομοθετικών ενεργειών είναι η επιδίωξη της μείωσης του κινδύνου αυτών των κυβερνοεπιθέσεων. Κάθε φορά που γίνεται χρήση μιας τεχνολογικής συσκευής, υπάρχει ο κίνδυνος κυβερνοεπίθεσης. Για το λόγο αυτό, υπάρχει ανάγκη άλλα και υποχρέωση να ενισχυθούν επαρκώς η ασφάλεια εναντίον τέτοιου είδους πιθανών απειλών, κάτι που ξεκίνησε σταδιακά να επιτυγχάνεται με την ανάπτυξη της Κυβερνοασφάλειας (Von Solms & Van Niekerk, 2013).

Βάση του ISO/IEC 27032:2012 η κυβερνοασφάλεια ορίζεται ως η προστασία της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών στον Κυβερνοχώρο. Η κυβερνοασφάλεια αποτελείται από μια δεσμίδα μέτρων, με κάποια από αυτά να είναι τεχνολογικής φύσεως, ενώ αλλά όχι. Πρωτεύων στόχος της κυβερνοασφάλειας είναι να ελαχιστοποιήσει την απειλή από τις κυβερνοεπιθέσεις (Von Solms & Van Niekerk, 2013).

Γενικότερα η κυβερνοασφάλεια έχει 3 βασικούς στόχους (Sun et al., 2018):

- **Εμπιστευτικότητα:** Οι πληροφορίες θα πρέπει να είναι προσβάσιμες μόνο σε όσους έχουν την κατάλληλη θέση στην ιεραρχία ενός οργανισμού.
- **Ακεραιότητα:** Διασφάλιση της ακεραιότητας και της εγκυρότητας των πληροφοριών.

- **Διαθεσιμότητα:** Οι υπηρεσίες παροχής πληροφοριών θα πρέπει να είναι πλήρως διαθέσιμες οποιαδήποτε χρονική στιγμή.

Στο πλαίσιο αυτής της εργασίας θα καταγράψουμε τις σύγχρονες απειλές τις οποίες καλείται να αντιμετωπίσει ο τομέας της κυβερνοασφάλειας. Θα αναφερθούμε σε απειλές που πλήττουν την εμπιστευτικότητα των πληροφοριών, όπως το σχετικό παράδειγμα της BEC, όπου η επίθεση χρησιμοποιείται για την απόκτηση πρόσβασης σε λογαριασμό υψηλόβαθμου στελέχους με απώτερο σκοπό την κλοπή εμπιστευτικών πληροφοριών ή χρημάτων (Al-Musib et al., 2021). Επιπλέον, θα γίνει αναφορά και σε επιθέσεις που στοχεύουν στην ακεραιότητα των πληροφοριών όπως οι επιθέσεις παραπληροφόρησης. Μετέπειτα θα εξεταστούν οι επιθέσεις που αφορούν την διαθεσιμότητα πληροφοριών όπως οι DDoS επιθέσεις. Τέλος, θα παρουσιαστούν μια σειρά λύσεων τις οποίες μπορεί να λάβει ένας οργανισμός για να προστατέψει τα πληροφοριακά συστήματά του.

1.1.1. Στόχοι Κυβερνοασφάλειας

Η έννοια της «εμπιστευτικότητας» αναφέρεται στη διατήρηση των εξουσιοδοτημένων περιορισμών πρόσβασης και αποκάλυψης, που περιλαμβάνει τη διαφύλαξη του προσωπικού απορρήτου και των ιδιοκτησιακών πληροφοριών , καθώς και των μέσων που χρησιμοποιηθούν για την επίτευξη.(CSRC Content Editor, 2023). Αυτή η έννοια συνδέεται στενά με την ασφάλεια στον κυβερνοχώρο, καθιστώντας αναγκαία τον έλεγχο της πρόσβασης σε προστατευμένες πληροφορίες. Πρέπει να εφαρμοστεί μια σειρά μέτρων για να διασφαλιστεί ότι συγκεκριμένα άτομα έχουν πρόσβαση σε προστατευμένες πληροφορίες, ενώ η πρόσβαση απαγορεύεται σε ακατάλληλα άτομα. Οι παραβιάσεις του απορρήτου μπορεί να έχουν ως αποτέλεσμα την απώλεια προσωπικών δεδομένων και την αποκάλυψη εμπιστευτικών πληροφοριών στο ευρύ κοινό ή σε ανεπιθύμητα πρόσωπα, με ευρύ φάσμα συνεπειών, όπως νομικές και οικονομικές επιπτώσεις, καθώς και επιπτώσεις στο κοινωνικό υπόβαθρο ενός οργανισμού (Lehto, 2013).

Για να διασφαλιστεί η προστασία του απορρήτου, είναι απαραίτητο να οριστούν οι προστατευόμενες πληροφορίες και να καθιερωθεί διαβαθμισμένη πρόσβαση τόσο εντός όσο και εκτός ενός οργανισμού. Για παράδειγμα, τα άτομα στο τμήμα IT ενός οργανισμού δεν θα πρέπει να έχουν πρόσβαση σε οικονομικά ή νομικά έγγραφα. Επιπλέον, όλα τα άτομα θα πρέπει να έχουν πρόσβαση στις πληροφορίες που απαιτούνται για την ολοκλήρωση της εργασίας τους (Sun et al., 2018).

Από την άλλη πλευρά, η <<ακεραιότητα>> είναι η προστασία που προσφέρει η κυβερνοασφάλεια έναντι κακόβουλων ενεργειών που στοχεύουν σε μη εξουσιοδοτημένες αλλαγές ή καταστροφή πληροφοριών, με σκοπό τη διασφάλιση τις αυθεντικότητας και ποιότητας τους. Η διασφάλιση ότι οι πληροφορίες δεν μπορούν να τροποποιηθούν με μη ανιχνεύσιμο τρόπο εγγυάται την ακεραιότητα και την πληρότητα των πληροφοριών και την ορθή λειτουργία των συστημάτων πληροφορικής. Για τη διασφάλιση της ακεραιότητας, πρέπει να καθιερωθεί διαβαθμισμένη πρόσβαση σε όλα τα επίπεδα συστήματος, έτσι ώστε οι χρήστες να μπορούν να τροποποιούν μόνο τις πληροφορίες για να διασφαλίσουν ότι έχουν την κατάλληλη πρόσβαση (Galiveeti et al., 2021). Επιπλέον, είναι σημαντικό να καταγράφονται όλες οι αλλαγές πληροφοριών που πραγματοποιούνται από τους χρήστες

χρονολογικά για λόγους διαφάνειας και εποπτείας. Εκτός από τις ενέργειες κατά των κακόβουλων δραστηριοτήτων, είναι εξίσου σημαντικό να αποτραπούν ακούσιες αλλαγές που μπορεί να προκύψουν από σφάλματα χρήστη ή ακόμα και την απώλεια πληροφοριών λόγω τεχνικών ζητημάτων (Sun et al., 2018).

Η <<διαθεσιμότητα>> είναι η ικανότητα ενός οργανισμού να παρέχει συνεχείς και αξιόπιστη πρόσβαση καθώς και χρήση των πληροφορίων που διαχειρίζεται. Είναι κρίσιμη για την αποτελεσματική λειτουργία και τη χρηστικότητά του. Η μη διαθεσιμότητα ενός συστήματος έχει αρνητικές επιπτώσεις σε έναν οργανισμό, με αποτέλεσμα απώλεια κερδών, δυσαρέσκεια πελατών ή συνεργατών και βλάβη στη φήμη του οργανισμού. Ως αποτέλεσμα, είναι σημαντικό να ληφθούν μέτρα για την αποφυγή διακοπής της διαθεσιμότητας από κακόβουλες ενέργειες. Ωστόσο, εκτός από αυτό, θα πρέπει επίσης να ληφθούν μέτρα για την αποφυγή διακοπής από οποιαδήποτε βλάβη στον εξοπλισμό (Galiveeti et al., 2021).

1.2 Ερευνητικός Στόχος

Λαμβάνοντας υπόψη το παραπάνω θεωρητικό πλαίσιο, κύριος σκοπός της παρούσας εργασίας είναι η καταγραφή και ανάλυση των σύγχρονων απειλών στον τομέα της κυβερνοασφάλειας, καθώς και πιθανών λύσεων για καθεμία από αυτές τις απειλές. Όπως αναφέρθηκε, η κυβερνοασφάλεια είναι ζωτικής σημασίας επειδή προστατεύει όλα τα δεδομένα και τις υπηρεσίες από κλοπή, ζημιά και άλλες κακόβουλες δραστηριότητες. Αυτό περιλαμβάνει δεδομένα κρίσιμα για τη λειτουργία μιας επιχείρησης, δεδομένα που προστατεύονται από το προσωπικό απόρρητο και την προσβασιμότητα και την ακεραιότητα μιας υπηρεσίας που μπορεί να προσφέρει μια εταιρεία. Ως εκ τούτου, ο εντοπισμός πιθανών απειλών και οι τρόποι αντιμετώπισής τους είναι ιδιαίτερα σημαντικός. Επιπλέον, έμφαση θα δοθεί σε νέες απειλές που έχουν εμφανιστεί τα τελευταία χρόνια, όπως επιθέσεις παραπληροφόρησης, ψευδούς παραπληροφόρησης, deepfakes και χρήση spyware από οργανισμούς για την παρακολούθηση των εργαζομένων τους. Τέλος, η παρούσα εργασία θα ασχοληθεί με τη δημιουργία ενός σχεδίου δράσης που θα μπορούσε να ακολουθήσει μια επιχείρηση ή οργανισμός για να μεγιστοποιήσει την ασφάλειά του.

ΚΕΦΛΑΙΟ 2. ΜΕΛΕΤΗ ΥΦΙΣΤΑΜΕΝΩΝ ΚΑΙ ΝΕΩΝ ΑΠΕΙΛΩΝ

Ως απειλή στον κυβερνοχώρο ορίζεται κάθε πιθανή επίθεση που στοχεύει σε μη εξουσιοδοτημένη πρόσβαση σε δεδομένα, διακοπή ψηφιακών υπηρεσιών ή βλάβη πληροφοριών. Οι απειλές στον κυβερνοχώρο μπορεί να προέρχονται από διάφορες οντότητες, όπως βιομηχανικούς κατασκόπους, χακτιβιστές, τρομοκράτες, εχθρικά έθνη, εγκληματικές οργανώσεις, χάκερ και μυστικούς (Thakur et al., 2015).

Η έκθεση ENISA για το 2021 χωρίζει τις απειλές σε 8 ομάδες (ENISA, 2021):

1. Ransomware
2. Κακόβουλο λογισμικό
3. Cryptojacking
4. Απειλές μέσω ηλεκτρονικού ταχυδρομείου
5. Απειλές κατά των Δεδομένων
6. Απειλές κατά της διαθεσιμότητας και της ακεραιότητας
7. Παραπληροφόρηση-Ψευδή πληροφόρηση
8. Μη Κακόβουλες Απειλές

Εκτός από τον ENISA, υπάρχουν και άλλες κατηγοριοποιήσεις, όπως αυτή της CISCO, γνωστής κατασκευάστριας δικτυακού εξοπλισμού, η οποία κατηγοριοποιεί τις απειλές ως εξής (Cisco Umbrella, 2023):

1. Κακόβουλο λογισμικό
2. Εντολή και έλεγχος επανάκλησης
3. Τομείς που εμφανίστηκαν πρόσφατα
4. Επιθέσεις phishing
5. Κρυπτοεξόρυξη
6. Δυναμικό DNS
7. Δυνητικά επιβλαβείς τομείς
8. VPN Tunneling DNS

Μια άλλη κατηγοριοποίηση είναι αυτή που χρησιμοποιεί η αυστραλιανή κυβέρνηση. Αυτή η κατηγοριοποίηση βασίζεται στη συχνότητα με την οποία έχουν παρατηρήσει αυτές τις επιθέσεις (Cyber.gov.au, 2023):

1. Κρυπτοεξόρυξη
2. Διαρροή δεδομένων
3. Άρνηση παροχής υπηρεσιών
4. Hacking
5. Κλοπή ταυτότητας
6. Κακόβουλοι Insiders
7. Κακόβουλο λογισμικό
8. Ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος
9. Ransomware
10. Απάτες
11. Κακόβουλο λογισμικό κελύφους Ιστού

Μια άλλη κατηγοριοποίηση είναι αυτή των Solarwinds. Αυτή η κατηγοριοποίηση βασίζεται στον στόχο της επίθεσης (SolarWinds, 2023):

1. Απειλές χρηστών
    i) Spear Phishing
    ii) Προνομιακή Διαχείριση Λογαριασμού
2. Απειλές Εφαρμογών
    i) Εφαρμογές Ιστού XSS
    ii) SQL Injections
3. Απειλές για τις υποδομές
    i) Botnets
    ii) DDOS

Υπάρχει επίσης η κατηγοριοποίηση του Exabeam (Cassetto, 2023):

1. Επίθεση κακόβουλου λογισμικού
2. Επιθέσεις κοινωνικής μηχανικής
3. Επιθέσεις στην αλυσίδα εφοδιασμού λογισμικού
4. Προηγμένες επίμονες απειλές
5. Κατανεμημένη άρνηση υπηρεσίας
6. Άνθρωπος στη μέση
7. Επιθέσεις κωδικού πρόσβασης

Υπάρχει επίσης η κατηγοριοποίηση των λύσεων ασφάλειας Datto (Datto Security Solutions, 2023):

1. Κακόβουλο λογισμικό
2. Phishing
3. Ανθρωπος στη μέση
4. Άρνηση παροχής υπηρεσιών
5. SQL Injection
6. Zero-Day Exploit
7. Επιθέσεις κωδικού πρόσβασης
8. Διαδικτυακή δέσμη ενεργειών
9. Rootkits
10. Επιθέσεις στο Διαδίκτυο των Πραγμάτων

Η κατηγοριοποίηση που επιλέγεται για την παρούσα εργασία βασίζεται στα προαναφερθέντα και στοχεύει να είναι όσο το δυνατόν πιο ολοκληρωμένη. Για τον λόγο αυτό επιλέγονται κατηγορίες που είναι πάντα σχετικές (κακόβουλο λογισμικό, απειλές ηλεκτρονικού ταχυδρομείου, μη κακόβουλες απειλές), κατηγορίες που επηρεάζουν τις βασικές αρχές ασφάλειας (απειλές κατά της εμπιστευτικότητας, απειλές κατά της διαθεσιμότητας και ακεραιότητας) καθώς και νέους τύπους απειλών (ransomware, cryptojacking, παραπληροφόρηση-παραπληροφόρηση). Επιπλέον, προσθέτετε η κατηγορία των Προηγμένων Μόνιμων Απειλών, η οποία είναι ιδιαίτερα σημαντική για οργανισμούς που συνεργάζονται στενά με κυβερνητικές δομές. Τέλος, εξετάζονται επίσης νέες κατηγορίες επιθέσεων σε συσκευές Internet of Things και Virtualization, οι οποίες έχουν ως εξής:

1. Ransomware
2. Κακόβουλο λογισμικό
3. Cryptojacking
4. Απειλές μέσω ηλεκτρονικού ταχυδρομείου
5. Απειλές κατά της εμπιστευτικότητας
6. Απειλές κατά της διαθεσιμότητας και της ακεραιότητας
7. Παραπληροφόρηση-παραπληροφόρηση
8. Μη Κακόβουλες Απειλές

9. Προηγμένες επίμονες απειλές
10. Επιθέσεις στο Διαδίκτυο των Πραγμάτων
11. Virtualization

Όπως μπορούμε να δούμε, η κατηγοριοποίησή μας είναι πιο ολοκληρωμένη σε σύγκριση με τις άλλες. Περιλαμβάνει όλους τους πιθανούς τύπους απειλών που μπορεί να αντιμετωπίζει ένας οργανισμός σε καθημερινή βάση.

2.1 Ransomware

Οι επιθέσεις ransomware είναι ένας τύπος κακόβουλης επίθεσης που στοχεύει στην κρυπτογράφηση των δεδομένων ενός οργανισμού και στην απαίτηση πληρωμής για την επιστροφή της πρόσβασης. Το Ransomware είναι μια σύγχρονη απειλή που έχει αποτελέσει τη βάση για πολλές επιθέσεις στον κυβερνοχώρο που έχουν κερδίσει την ευρύτερη προσοχή του κοινού. Η σημασία και ο αντίκτυπος αυτού του τύπου απειλής αποδεικνύεται από μια σειρά σχετικών πρωτοβουλιών πολιτικής της Ευρωπαϊκής Ένωσης και άλλων κρατών παγκοσμίως, όπως οι κυρώσεις που επιβλήθηκαν από την ΕΕ το 2020 κατά των επιθέσεων στον κυβερνοχώρο (ENISA, 2021· European Council, 2020).

Αρχικά γνωστές ως «κρυπτοϊικός εκβιασμός» (cryptoviral extortion), οι επιθέσεις Ransomware αναπτύχθηκαν από τους Moti Young και Adam Young του Πανεπιστημίου Columbia. Η ιδέα γεννήθηκε στα πανεπιστήμια και αντιπροσώπευε την πρόοδο, τη δύναμη και τη δημιουργία σύγχρονων εργαλείων κρυπτογράφησης. Ο ιός περιείχε το δημόσιο κλειδί του εισβολέα και κρυπτογραφούσε τα αρχεία του θύματος. Το κακόβουλο λογισμικό έδωσε εντολή στο θύμα να στείλει το ασύμμετρο κρυπτογραφημένο κείμενο, ένα κρυπτογραφημένο μήνυμα κειμένου, για αποκωδικοποίηση, επιστρέφοντας το κλειδί αποκρυπτογράφησης έναντι αμοιβής (Malwarebytes, 2022).

Με την πάροδο του χρόνου, οι εισβολείς αύξησαν τη δημιουργικότητά τους, αναζητώντας μεθόδους πληρωμής που είναι εξαιρετικά δύσκολο να ακολουθηθούν, επιτρέποντάς τους να παραμείνουν ανώνυμοι. Με την άνοδο των κρυπτονομισμάτων, ο αριθμός τέτοιων επιθέσεων έχει αυξηθεί δραματικά, καθώς η ανωνυμία τους καθιστά αρκετά δύσκολη την παρακολούθησή τους. Ένας επιπλέον λόγος για την αύξηση των επιθέσεων Ransomware είναι η απομακρυσμένη εργασία. Η πανδημία ενίσχυσε αυτό το νέο είδος εργασίας παγκοσμίως. Μια ομάδα εργαζομένων στο σπίτι είναι πολύ πιο ευάλωτη σε απειλές. Οι οικιακοί χρήστες δεν διαθέτουν συστήματα ασφαλείας εταιρικού επιπέδου για την προστασία τους από εξειδικευμένες επιθέσεις και πολλοί χρησιμοποιούν τις συσκευές τους για τις επαγγελματικές τους ανάγκες. Το σύγχρονο Ransomware είναι εξοπλισμένο με σενάρια για τη σάρωση ενός δικτύου για ευάλωτες συσκευές. Ως εκ τούτου, ακόμη και προσωπικές συσκευές όπως τα κινητά τηλέφωνα, που συνήθως διαθέτουν πιο ήπια συστήματα ασφαλείας, μπορούν να χρησιμοποιηθούν ως αφετηρία για τη διάδοση του ιού.

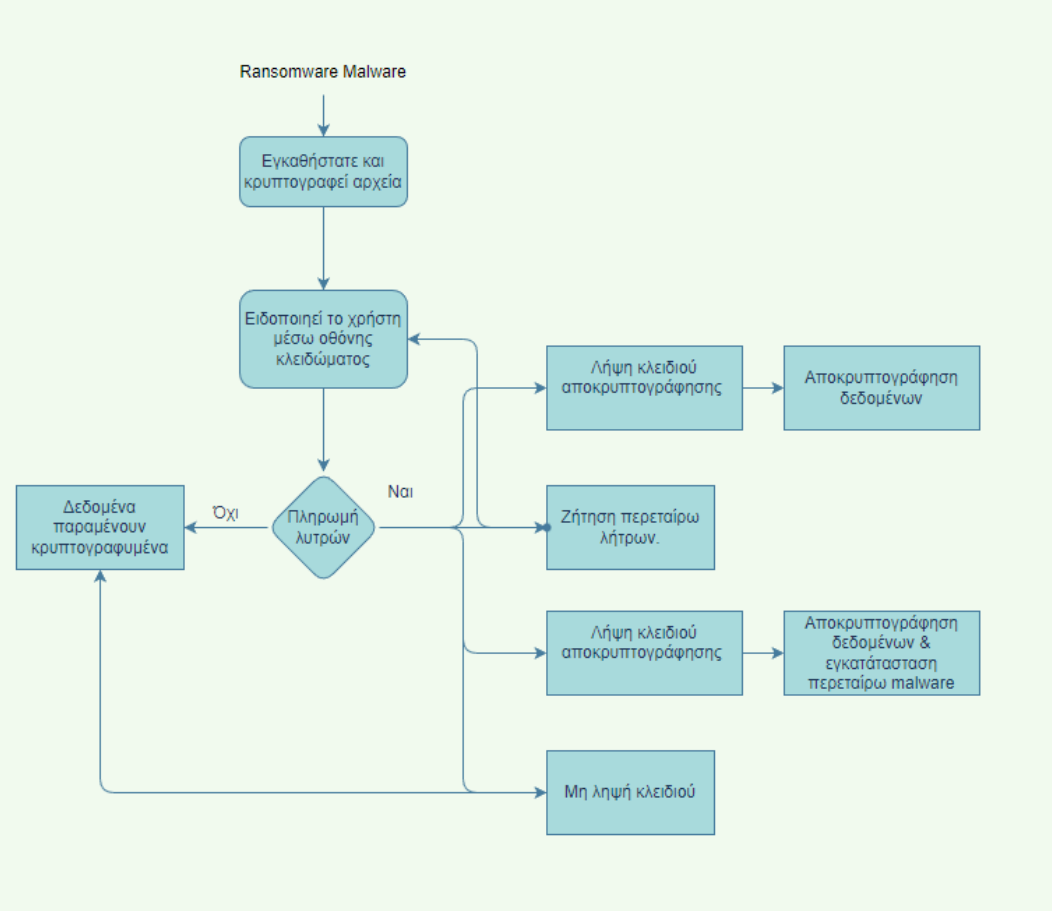
Κατά συνέπεια, οι υπολογιστές που χρησιμοποιούνται για επαγγελματική εργασία μπορεί να επηρεαστούν (Malwarebytes, 2022· Trellix, 2023).

Μια τυπική επίθεση Ransomware αποτελείται από δύο στοιχεία, τον κρυπτογράφηση και το κλείδωμα οθόνης. Ο κρυπτογραφητής κρυπτογραφεί δεδομένα στο σύστημα, καθιστώντας τα άχρηστα χωρίς το κλειδί αποκρυπτογράφησης. Το κλείδωμα οθόνης αποκλείει την πρόσβαση σε ένα σύστημα μέσω μιας «οθόνης κλειδώματος», ειδοποιώντας τον χρήστη ότι το σύστημα είναι κρυπτογραφημένο (Malwarebytes, 2022).

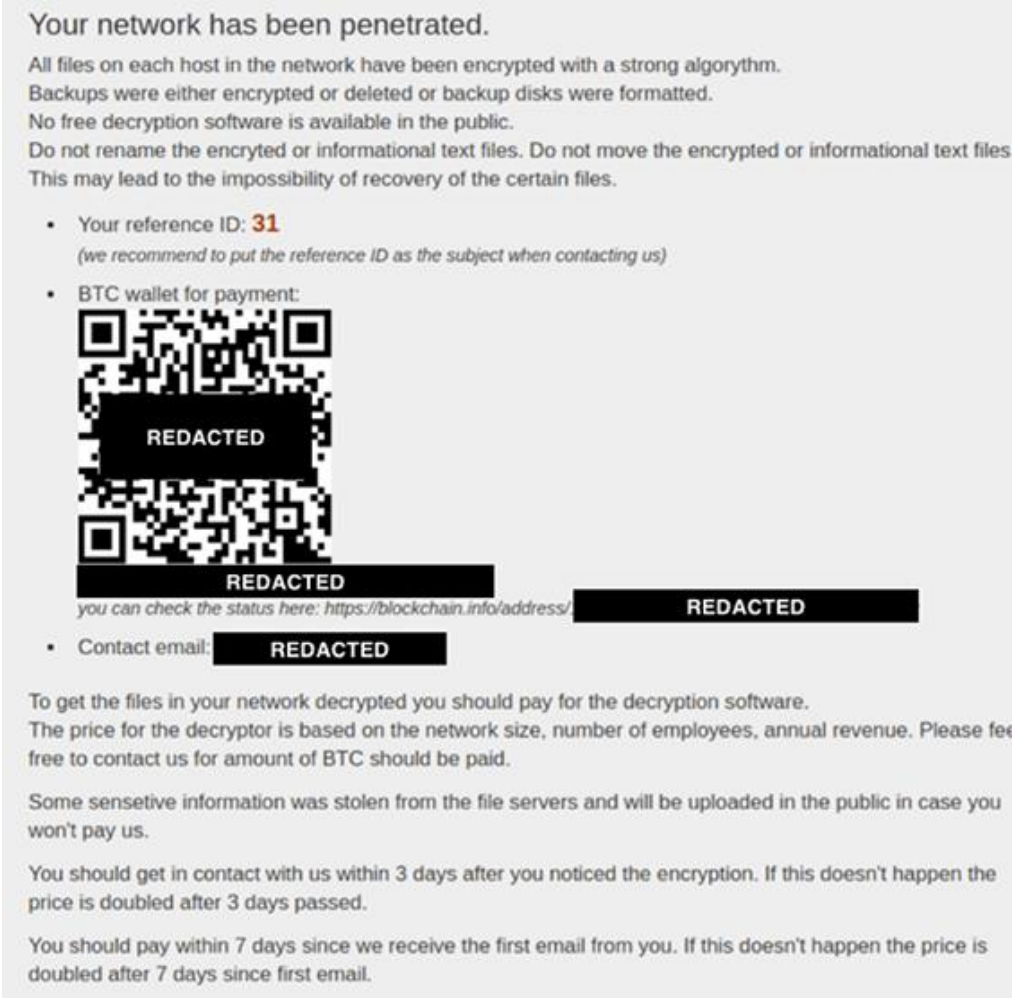
Δύο άλλοι διαδεδομένοι τύποι Ransomware είναι το Master Boot Record (MBR) ransomware και το Mobile device ransomware. Στην πρώτη, ένα τμήμα του σκληρού δίσκου που επιτρέπει την εκκίνηση του λειτουργικού συστήματος είναι κρυπτογραφημένο, καθιστώντας το σύστημα ανίκανο να εκκινήσει. Αντίθετα, εμφανίζεται μια «οθόνη κλειδώματος». Στο τελευταίο, τα smartphones μπορούν να μολυνθούν μέσω λήψεων ή ψεύτικων εφαρμογών που υποδύονται δημοφιλείς υπηρεσίες όπως το Adobe Flash ή ένα πρόγραμμα προστασίας από ιούς (The No More Ransom Project, 2023).

Και στους τρεις τύπους, τα θύματα συχνά ειδοποιούνται μέσω μιας «οθόνης κλειδώματος» να αγοράσουν ένα κρυπτονόμισμα με το οποίο θα πληρώσουν τα λύτρα. Όταν πληρωθούν τα λύτρα, οι «πελάτες» λαμβάνουν το κλειδί αποκρυπτογράφησης και μπορούν να επιχειρήσουν να αποκρυπτογραφήσουν τα αρχεία τους. Ωστόσο, η αποκρυπτογράφηση δεν είναι πάντα εγγυημένη. Μερικές φορές, τα θύματα δεν λαμβάνουν ποτέ κλειδιά ή ζητούνται περαιτέρω λύτρα. Άλλες φορές, το κακόβουλο λογισμικό εγκαθίσταται ακόμη και μετά την πληρωμή των λύτρων (Malwarebytes, 2022).

Εικόνα 1. Διαγραμματική απεικόνιση Ransomware



Εικόνα 2. Παράδειγμα οθόνης κλειδώματος από Ransomware BitPaymer,4 Δεκεμβρίου 2022,<https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-examples/>



Αν και αρχικά στόχευαν κυρίως προσωπικούς υπολογιστές, οι επιθέσεις ransomware στοχεύουν όλο και περισσότερο τις επιχειρήσεις, καθώς είναι πιο πρόθυμες να πληρώσουν σημαντικά χρηματικά ποσά για να ξεκλειδώσουν κρίσιμα δεδομένα. Οι επιθέσεις σε επιχειρήσεις συνήθως ξεκινούν με ένα κακόβουλο email. Ένας ανυποψίαστος χρήστης ανοίγει ένα συνημμένο ή κάνει κλικ σε έναν κακόβουλο σύνδεσμο. Σε αυτό το σημείο, το πρόγραμμα ransomware εγκαθίσταται στο λειτουργικό σύστημα και κρυπτογραφεί αρχεία στο σύστημα του χρήστη. Μετά την κρυπτογράφηση των δεδομένων, το ransomware εμφανίζει ένα μήνυμα στην οθόνη με οδηγίες, εξηγώντας στον χρήστη τι συνέβη και ότι πρέπει να πληρώσουν τους εισβολείς για να ανακτήσουν την πρόσβαση στα δεδομένα τους.

Όπως αναφέρθηκε προηγουμένως, οποιαδήποτε συσκευή είναι συνδεδεμένη σε ένα δίκτυο μπορεί ενδεχομένως να στοχευτεί από ransomware. Στην περίπτωση ενός δικτύου που

ανήκει σε επιχειρήσεις, το ransomware μπορεί να κρυπτογραφήσει σημαντικά έγγραφα και αρχεία συστήματος που μπορούν να ακινητοποιήσουν τις υπηρεσίες και την παραγωγικότητα. Οι δημιουργοί ransomware τροποποιούν συνεχώς τον κώδικά τους για να αποφύγουν τον εντοπισμό. Μερικές νέες τεχνικές που έχουν αναπτυχθεί περιλαμβάνουν:

- **DLL side loading:** Το Ransomware προσπαθεί να κρυφτεί από τον εντοπισμό του συστήματος ασφαλείας χρησιμοποιώντας αρχεία τύπου DLL. Εκμεταλλεύεται τον χειρισμό αρχείων DLL από τα Microsoft Windows για να εμφανίζεται ως "κανονική" δραστηριότητα. Σε αυτές τις επιθέσεις, το κακόβουλο λογισμικό τοποθετεί ένα πλαστό αρχείο DLL στο φάκελο WinSxS, έτσι ώστε το λειτουργικό σύστημα να το φορτώνει αντί για το κανονικό αρχείο. Τα Windows χρησιμοποιούν το φάκελο WinSxS για την αποθήκευση αρχείων που σχετίζονται με διάφορες λειτουργίες του λειτουργικού συστήματος (Malwarebytes, 2022· Mandiant, 2023).
- **Web servers as Targets**: Σε ένα κοινόχρηστο περιβάλλον φιλοξενίας, μπορούν να επηρεαστούν όλοι οι ιστότοποι σε έναν διακομιστή. Γνωστά τρωτά σημεία στα Συστήματα Διαχείρισης Περιεχομένου χρησιμοποιούνται για την εισαγωγή ransomware σε υπηρεσίες web (Malwarebytes, 2022· The No More Ransom Project, 2023).
- **Spear-phishing**: Αντί να στέλνουν κακόβουλο λογισμικό σε χιλιάδες στόχους, οι εισβολείς ερευνούν πιθανούς στόχους που μπορεί να έχουν πρόσβαση σε δίκτυα υψηλής αξίας (Malwarebytes, 2022)..
- **Ransomware ως υπηρεσία (RaaS)**: Είναι ένα οικονομικό μοντέλο κυβερνοεγκλήματος που επιτρέπει στους δημιουργούς κακόβουλου λογισμικού να κερδίσουν χρήματα από τις δημιουργίες τους χωρίς να τις διανέμουν προσωπικά. Εγκληματίες χωρίς τεχνική εκπαίδευση αγοράζουν το κακόβουλο λογισμικό και εκτελούν επιθέσεις, πληρώνοντας ένα ποσοστό στους δημιουργούς. Έτσι, οι δημιουργοί εκτίθενται σε λιγότερους κινδύνους, καθώς οι πελάτες κάνουν το μεγαλύτερο μέρος της δουλειάς (Trellix, 2023).

2.2 Malware

Όπως ορίζεται από τον ENISA (2021), το κακόβουλο λογισμικό είναι ένας τύπος λογισμικού που εκτελεί μη εξουσιοδοτημένες εργασίες που θα επηρεάσουν αρνητικά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα ενός συστήματος. Το κακόβουλο λογισμικό είναι ένας γενικός όρος που περιλαμβάνει όλα τα κακόβουλα προγράμματα που έχουν σχεδιαστεί για να προκαλέσουν βλάβη σε μια συσκευή, ένα δίκτυο ή μια υπηρεσία. Οι εγκληματίες χρησιμοποιούν κακόβουλο λογισμικό για την εξαγωγή δεδομένων που μπορούν να χρησιμοποιηθούν για εκβιασμό και οικονομικό κέρδος. Οι κλεμμένες πληροφορίες μπορεί να είναι νομισματικά, αρχεία υγείας, προσωπικά email και κωδικοί πρόσβασης. Οι επιλογές για το ποιες πληροφορίες μπορούν να κλαπούν είναι ατελείωτες (McAfee, 2023).

Εκτός από το οικονομικό όφελος, το κακόβουλο λογισμικό χρησιμοποιείται για άλλους σκοπούς, όπως η κλοπή προσωπικών πληροφοριών, με απώτερο στόχο την κλοπή ταυτότητας. Επιπλέον, τα μολυσμένα συστήματα μπορούν να χρησιμοποιηθούν ως bot σε επιθέσεις DDoS. Υπάρχουν πολλοί διαφορετικοί τύποι κακόβουλου λογισμικού, ο καθένας με έναν μακρινό στόχο. Αυτά περιλαμβάνουν:

Viruses: Οι ιοί είναι ο πιο κοινός τύπος κακόβουλου λογισμικού. Επισυνάπτουν τον κακόβουλο κώδικα σε ασφαλή κώδικα και περιμένουν έναν ανυποψίαστο χρήστη ή μια αυτοματοποιημένη λειτουργία να τους εκτελέσει. Παρόμοια με τους βιολογικούς ιούς, μπορούν να εξαπλωθούν γρήγορα και να προκαλέσουν ζημιά σε κρίσιμες λειτουργίες του συστήματος, να καταστρέψουν αρχεία και να απαγορεύσουν στους χρήστες την πρόσβαση στους υπολογιστές τους. Συνήθως περιέχονται σε ένα εκτελέσιμο αρχείο, αλλά μπορούν επίσης να επισυναφθούν σε βιβλιοθήκες όπως τα DLL (McAfee, 2023).

Worms: Τα σκουλήκια ονομάζονται από τον τρόπο που μολύνουν τα συστήματα. Ξεκινώντας από ένα μολυσμένο σύστημα, διαδίδονται μέσω του δικτύου, μολύνοντας όλες τις συνδεδεμένες συσκευές. Εκμεταλλεύονται ευπάθειες λογισμικού ή δικτύου και δεν απαιτούν καμία ενέργεια από τον χρήστη. Τα σκουλήκια δικτύου, όπως είναι επίσης γνωστά, μπορούν να προκαλέσουν διάφορες ζημιές, όπως κλοπή πληροφοριών, δημιουργία backdoor για μελλοντική πρόσβαση σε ένα σύστημα και καταστροφή αρχείων (McAfee, 2023).

Scareware: Το Scareware είναι ένας τύπος κακόβουλου λογισμικού που χρησιμοποιούν οι εγκληματίες του κυβερνοχώρου για να φοβίσουν τους χρήστες να πιστέψουν ότι οι υπολογιστές τους είναι μολυσμένοι με ιούς για να τους πείσουν να αγοράσουν ψεύτικο λογισμικό. Σε μια τυπική επίθεση scareware, καθώς ο χρήστης περιηγείται στο διαδίκτυο, μπορεί να δει μηνύματα όπως "Κίνδυνος: Ο υπολογιστής σας έχει μολυνθεί" ή "Έχετε έναν ιό". Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν τέτοιες τακτικές για να φοβίσουν τους χρήστες και να τους οδηγήσουν να αγοράσουν και να εγκαταστήσουν πραγματικά κακόβουλες εφαρμογές (McAfee, 2023).

Spyware: Το spyware αναφέρεται σε κακόβουλο λογισμικό που είναι εγκατεστημένο σε ένα σύστημα υπολογιστή εν αγνοία του χρήστη και παρακολουθεί και μεταδίδει προσωπικά δεδομένα που σχετίζονται με τις συνήθειες περιήγησης του χρήστη ή τη χρήση του συστήματος. Το λογισμικό κατασκοπείας μπορεί να χρησιμοποιηθεί για την παρακολούθηση όλων των μορφών επικοινωνίας σε μια μολυσμένη συσκευή και από υπηρεσίες ασφαλείας ή κυβερνήσεις για την παρακολούθηση ευαίσθητων περιβαλλόντων ή εγκληματικών ερευνών (McAfee, 2023). Τέτοια προγράμματα βρίσκουν χρήση σε χώρους εργασίας για την παρακολούθηση της δραστηριότητας των εργαζομένων, κυρίως στις Ηνωμένες Πολιτείες. Ωστόσο, στην Ευρώπη, τέτοια προγράμματα υπόκεινται στους νόμους περί απορρήτου και προστασίας προσωπικών δεδομένων και, ως εκ τούτου, δεν μπορεί να παρακολουθείται κάθε ενέργεια ενός υπαλλήλου. Η υπόθεση Bărbulescu είναι ένα παράδειγμα όπου το Ευρωπαϊκό Δικαστήριο Ανθρωπίνων Δικαιωμάτων έκρινε ότι η απόλυση ενός υπαλλήλου έγινε μέσω παρακολούθησης που υπερέβαινε τα όρια των προσωπικών δεδομένων (ΕΣΔΑ, 2023).

- ***Adware***: Το Adware είναι λογισμικό που εμφανίζει διαφημίσεις στον χρήστη, συνήθως με αντάλλαγμα τη χρήση συγκεκριμένου λογισμικού ή υπηρεσιών χωρίς πληρωμή. Το Adware συχνά εμφανίζει αναδυόμενα παράθυρα ή banner όταν ο χρήστης ενεργεί, αλλά μπορεί επίσης να είναι δούρειος ίππος για την εγκατάσταση άλλων επιβλαβών μορφών κακόβουλου λογισμικού (McAfee, 2023).
- ***Trojans***: Οι Trojans είναι ιοί πολλαπλών χρήσεων που προσποιούνται ότι είναι αβλαβείς εφαρμογές, εξαπατώντας τους χρήστες να τις κατεβάσουν και να τις χρησιμοποιήσουν. Μόλις ενεργοποιηθούν, οι Trojans μπορούν να κλέψουν

προσωπικά δεδομένα, να διαταράξουν τις λειτουργίες του υπολογιστή, να κατασκοπεύσουν τις δραστηριότητες των χρηστών και να εξαπολύσουν επιθέσεις (McAfee, 2023).

- ***Botnet:*** Τα botnet, συντομογραφία για τα "δίκτυα ρομπότ", είναι δίκτυα μολυσμένων υπολογιστών υπό τον έλεγχο ενός κεντρικού προγράμματος που χρησιμοποιεί διακομιστές εντολών και ελέγχου. Τα botnets είναι εξαιρετικά ευέλικτα και προσαρμόσιμα, ικανά να διατηρούν ανθεκτικότητα μέσω πολλών διακομιστών και να χρησιμοποιούν μολυσμένους υπολογιστές για τη διοχέτευση της κίνησης. Τα botnet είναι συνήθως οι στρατοί πίσω από τις σημερινές επιθέσεις DDoS (Palo Alto Networks, 2023).
- ***Rootkits***: Προγράμματα που παρέχουν πρόσβαση σε επίπεδο ρίζας στο λειτουργικό σύστημα ενός υπολογιστή, επιτρέποντας σε έναν κακόβουλο χρήστη να εγκαταστήσει πρόσθετα προγράμματα και γενικά να κάνει ό,τι θέλει με το σύστημα. Τα Rootkit ποικίλλουν στη δομή, γεγονός που καθιστά δύσκολο τον εντοπισμό τους. Μπορούν επίσης να κρυφτούν μέσα σε ένα λειτουργικό σύστημα, περιπλέκοντας περαιτέρω τον εντοπισμό τους (Palo Alto Networks, 2023).
- ***Remote Administration Tools (RAT)***: Προγράμματα που επιτρέπουν τον απομακρυσμένο έλεγχο του συστήματος. Ενώ αυτά τα εργαλεία δημιουργήθηκαν για την ικανοποίηση νόμιμων αναγκών, μπορούν να χρησιμοποιηθούν από κακόβουλες οντότητες. Τέτοια προγράμματα επιτρέπουν σε έναν εισβολέα να ελέγχει πλήρως ένα σύστημα, καθιστώντας δυνατή οποιαδήποτε ενέργεια μόλις αποκτηθεί πρόσβαση. Οι RAT είναι δύσκολο να εντοπιστούν, καθώς εκτελούν μη κακόβουλες λειτουργίες και η παρουσία τους στον υπολογιστή ενός χρήστη δεν θα εγείρει υποψίες (Palo Alto Networks, 2023).
- ***Fileless malware***: Ένας τύπος κακόβουλου λογισμικού που συνδέεται με μη κακόβουλα προγράμματα για να μολύνει έναν υπολογιστή. Σε αντίθεση με το παραδοσιακό κακόβουλο λογισμικό, το κακόβουλο λογισμικό χωρίς αρχεία δεν εγκαθίσταται ως πρόγραμμα. Αντίθετα, ενσωματώνει κώδικα σε μη κακόβουλα σενάρια προγραμμάτων και εκτελείται μαζί τους. Αυτό καθιστά ιδιαίτερα δύσκολη την αφαίρεσή τους, καθώς όχι μόνο δεν εντοπίζονται εύκολα, αλλά η αφαίρεσή τους μπορεί να απαιτεί απεγκατάσταση και επανεγκατάσταση του μολυσμένου

προγράμματος, προκαλώντας δυνητικά σοβαρά λειτουργικά προβλήματα σε έναν οργανισμό. Το παραδοσιακό λογισμικό προστασίας από ιούς συνήθως αναζητά "υπογραφές", συγκεκριμένες τεχνικές που χρησιμοποιούνται σε κακόβουλα προγράμματα. Ωστόσο, το κακόβουλο λογισμικό χωρίς αρχεία δεν αφήνει τέτοιο ίχνος (Trellix, 2023· Palo Alto Networks, 2023a).

- ***Αρχεία Polygot***: Τα αρχεία Polygot μπορούν να ανήκουν σε πολλούς τύπους αρχείων ταυτόχρονα. Για παράδειγμα, ένα αρχείο polygot θα μπορούσε να είναι ένα αρχείο PPT και JS, επιτρέποντάς του να ανοίγει από εφαρμογές που διαβάζουν οποιονδήποτε τύπο αρχείου. Αυτά τα αρχεία δεν είναι εγγενώς κακόβουλα, αλλά οι εγκληματίες του κυβερνοχώρου εισάγουν κακόβουλο κώδικα σε αυτά για να παρακάμψουν συστήματα ελέγχου τύπου αρχείου, τα οποία επιτρέπουν μόνο την εκτέλεση ή τη μεταφόρτωση συγκεκριμένων τύπων αρχείων σε έναν διακομιστή, συνήθως αρχεία DOC, GIF και JPEG. Ένα αρχείο Phar-Jpeg polygot, για παράδειγμα, θα μπορούσε να περάσει μέσα από ένα τέτοιο σύστημα, δεδομένου ότι είναι τύπου JPEG. Μόλις ανοίξει το αρχείο Phar, μπορεί να εκτελέσει μια επίθεση ένεσης αντικειμένου PHP (RSS, 2023· Li, 2019).

2.3 Cryptojacking

Το Cryptojacking, γνωστό και ως κρυφή εξόρυξη κρυπτονομισμάτων, είναι ένας τύπος εγκλήματος στον κυβερνοχώρο όπου ο δράστης χρησιμοποιεί κρυφά την επεξεργαστική ισχύ του συστήματος ενός χρήστη για να δημιουργήσει κρυπτονομίσματα. Το λογισμικό λειτουργεί στο παρασκήνιο με εξόρυξη κρυπτονομισμάτων ή κλοπή από πορτοφόλια κρυπτονομισμάτων. Οι χρήστες μπορούν να συνεχίσουν να χρησιμοποιούν τις συσκευές τους συνήθως, αλλά ενδέχεται να αντιμετωπίσουν χαμηλότερες επιδόσεις και καθυστερήσεις συστήματος. Με την άνοδο των κρυπτονομισμάτων και την υιοθέτησή τους από μια ολοένα αυξανόμενη μερίδα του πληθυσμού, έχει σημειωθεί αύξηση τέτοιων επιθέσεων.

Το κακόβουλο λογισμικό Cryptojacking ενσωματώνεται σε έναν υπολογιστή ή smartphone και χρησιμοποιεί τους πόρους του για την εξόρυξη κρυπτονομισμάτων. Τα κρυπτονομίσματα είναι ψηφιακά νομίσματα που έχουν τη μορφή «κερμάτων». Το πιο γνωστό είναι το Bitcoin, αλλά υπάρχουν πολλές άλλες μορφές κρυπτονομισμάτων, και ενώ μερικά έχουν μπει στον φυσικό κόσμο μέσω πιστωτικών καρτών ή άλλων μέσων, τα περισσότερα παραμένουν ψηφιακά (Kaspersky, 2023) (Interpol, 2023).

Τα κρυπτονομίσματα χρησιμοποιούν μια κατανεμημένη βάση δεδομένων, γνωστή ως blockchain, για να λειτουργήσουν. Το blockchain ενημερώνεται συχνά με πληροφορίες για όλες τις συναλλαγές πριν από την τελευταία ενημέρωση. Κάθε σύνολο πρόσφατων συναλλαγών συνδυάζεται σε ένα «μπλοκ» χρησιμοποιώντας πολύπλοκες μαθηματικές πράξεις. Για τη δημιουργία νέων μπλοκ, τα κρυπτονομίσματα βασίζονται σε χρήστες που παρέχουν υπολογιστική ισχύ για τη δημιουργία τους. Όσοι παρέχουν υπολογιστική ισχύ ανταμείβονται με κρυπτονομίσματα. Όσοι ανταλλάσσουν υπολογιστικούς πόρους με κρυπτονομίσματα ονομάζονται «miners». Τα μεγαλύτερα κρυπτονομίσματα χρησιμοποιούν μεγάλες «φάρμες» συστημάτων που τρέχουν αποκλειστικούς υπολογιστές για να ολοκληρώσουν τις απαραίτητες μαθηματικές πράξεις. Ωστόσο, αυτή η δραστηριότητα απαιτεί σημαντική ποσότητα ηλεκτρικής ενέργειας. για παράδειγμα, το δίκτυο Bitcoin χρησιμοποιεί περισσότερες από 73 TWh.

Ακολουθούν επιθέσεις cryptojacking, που πραγματοποιούνται από άτομα γνωστά ως cryptojackers. Αυτά τα άτομα επιδιώκουν να καρπωθούν τα οφέλη της εξόρυξης

κρυπτονομισμάτων χωρίς να επιβαρύνονται τα ίδια με το υψηλό κόστος παραγωγής. Αποφεύγοντας το κόστος του ακριβού υλικού εξόρυξης ή της ενέργειας που απαιτείται για την εξόρυξη, το cryptojacking δίνει τη δυνατότητα στους χάκερ να εξορύξουν κρυπτονομίσματα παρακάμπτοντας το υψηλό κόστος.

Υπάρχουν δύο κύριοι τρόποι με τους οποίους οι χάκερ μπορούν να εισέλθουν στο σύστημα ενός θύματος και να το χρησιμοποιήσουν για την εξόρυξη κρυπτονομισμάτων:

- Μέσω κακόβουλων συνδέσμων σε email που φορτώνουν τον κώδικα εξόρυξης στον υπολογιστή του θύματος.
- Μέσω ενός παραβιασμένου ιστότοπου ή μιας διαφήμισης που χρησιμοποιεί κώδικα JavaScript που εκτελείται αυτόματα όταν φορτωθεί στο πρόγραμμα περιήγησης του θύματος.

Και στις δύο περιπτώσεις, ο κώδικας τοποθετεί ένα σενάριο κρυπτογράφησης σε μια συσκευή που εκτελείται στο παρασκήνιο ενώ το θύμα εργάζεται. Εκτελεί πολύπλοκους μαθηματικούς υπολογισμούς και στέλνει τα αποτελέσματα σε έναν διακομιστή που ελέγχεται από τον χάκερ.

Σε αντίθεση με άλλα κακόβουλα προγράμματα, τα σενάρια κρυπτογράφησης δεν προκαλούν ζημιά στον υπολογιστή ή τα δεδομένα του θύματος, αλλά έχουν αρνητικές συνέπειες τόσο για τους πολίτες όσο και για τις επιχειρήσεις, όπως:

- Η χρήση του γραφείου βοήθειας και ο χρόνος που σπαταλά το τμήμα πληροφορικής για να βρει τι προκαλεί τη μειωμένη απόδοση και το κόστος πιθανής αντικατάστασης εξαρτημάτων.
- Αυξημένο ενεργειακό κόστος.

Ορισμένα σενάρια εξόρυξης κρυπτονομισμάτων έχουν δυνατότητες παρασίτων, επιτρέποντάς τους να μολύνουν άλλες συσκευές σε ένα δίκτυο και να ελέγχουν μια συσκευή για να δουν αν υπάρχει ήδη ανταγωνιστικό κακόβουλο λογισμικό εξόρυξης κρυπτονομισμάτων. Αν ναι, το απενεργοποιούν (ENISA, 2021).

2.4 E-mail Threats

Οι απειλές μέσω email αντιπροσωπεύουν μια μορφή κακόβουλης επίθεσης που στοχεύει στην εκμετάλλευση του ανθρώπινου παράγοντα και όχι των τεχνικών αδυναμιών ενός συστήματος. Τέτοιες επιθέσεις επιδιώκουν να χειραγωγήσουν άτομα για να εκπληρώσουν τις επιθυμίες του επιτιθέμενου χωρίς να τους ενημερώσουν για την κατάσταση. Μέσω αυτών των μέσων, οι εισβολείς μπορούν να εισάγουν κακόβουλο λογισμικό στο δίκτυο ενός οργανισμού ή να εξαπατήσουν τους χρήστες για οικονομικό όφελος.

Οι οργανισμοί αντιμετωπίζουν υψηλή απειλή παρά τις σημαντικές επενδύσεις στην εκπαίδευση προσωπικού και πελατών. Οι επιθέσεις ηλεκτρονικού ταχυδρομείου είναι από τις πιο διαδεδομένες και προσοδοφόρες μεθόδους που χρησιμοποιούν οι κακόβουλοι χρήστες για να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.

Οι παρακάτω είναι τύποι απειλών email:

Phishing: Οι τεχνικές phishing χρησιμοποιούν ψυχολογική χειραγώγηση για να πείσουν τους παραλήπτες να αποκαλύψουν ευαίσθητες πληροφορίες που μπορούν να χρησιμοποιηθούν για κακόβουλους σκοπούς, όπως η πώληση των δεδομένων τους. Μια επίθεση phishing αποτελείται συνήθως από έναν "αυθεντικό" αποστολέα και ένα κοινωνικά σχεδιασμένο μήνυμα, γεγονός που καθιστά δύσκολο για τους χρήστες που δεν γνωρίζουν τέτοιες απάτες να τους αναγνωρίσουν. Ο αποστολέας δημιουργεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου οπτικά και προφορικά, παρόμοια με τα μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από τον οργανισμό τον οποίο υποδύονται. Τα μηνύματα ηλεκτρονικού ψαρέματος ενδέχεται να περιέχουν συνημμένα κακόβουλου λογισμικού, συνδέσμους προς κακόβουλους ιστότοπους ή συνδυασμό.

Εξειδικευμένες τεχνικές, όπως το spear phishing, στοχεύουν συγκεκριμένα άτομα ή οργανισμούς. Σε αυτήν την περίπτωση, οι εγκληματίες του κυβερνοχώρου διεξάγουν εκτεταμένη έρευνα σε πιθανά θύματα για να κάνουν τα email τους να φαίνονται πιο αυθεντικά προσαρμόζοντάς τα στους στόχους τους. Η φαλαινοθηρία είναι μια παραλλαγή αυτής της προσέγγισης, η οποία στοχεύει άτομα υψηλού επιπέδου, όπως διευθύνοντες συμβούλους και πολιτικούς. Επιπλέον, υπάρχει το smishing, το οποίο χρησιμοποιεί SMS αντί

για email για παρόμοιους σκοπούς, και το vishing, το οποίο χρησιμοποιεί μέσα που βασίζονται στη φωνή.

Το QRishing είναι μια νέα τεχνική phishing που έχει εμφανιστεί τα τελευταία χρόνια. Λόγω των μέτρων κοινωνικής απόστασης κατά τη διάρκεια της πανδημίας, οι κωδικοί QR έχουν γίνει πιο διαδεδομένοι καθώς είναι εύκολοι στη χρήση και τη δημιουργία τους. Η αναγνώριση ενός πλαστού μηνύματος QR είναι πρόκληση, καθιστώντας αυτήν τη μέθοδο επίθεσης όλο και πιο δημοφιλής (Mimecast, 2023).

Το email είναι ένα πανταχού παρόν εργαλείο επικοινωνίας που έχει φέρει επανάσταση στον τρόπο αλληλεπίδρασης ατόμων και οργανισμών. Ωστόσο, καθώς η χρήση email συνεχίζει να αυξάνεται, αυξάνεται και ο αριθμός των απειλών που αντιμετωπίζουν οι χρήστες. Οι απειλές ηλεκτρονικού ταχυδρομείου μπορούν να κατηγοριοποιηθούν ευρέως σε τρεις κύριους τύπους: ανεπιθύμητη αλληλογραφία, πλαστογράφηση και συμβιβασμός email για επιχειρήσεις (BEC).

Spam: Το spam αναφέρεται σε ανεπιθύμητα και αυτόκλητα μηνύματα ηλεκτρονικού ταχυδρομείου που κατακλύζουν τα εισερχόμενα ενός χρήστη, συχνά για να προωθήσουν δόλια προγράμματα ή να πουλήσουν προϊόντα και υπηρεσίες. Ενώ έχουν αναπτυχθεί διάφορα φίλτρα και τεχνολογίες email για τον μετριασμό αυτής της απειλής, το spam παραμένει ένα σημαντικό ζήτημα για τους χρήστες email. Οι δύο κύριοι τύποι ανεπιθύμητων μηνυμάτων είναι τα περιοδικά ανεπιθύμητα μηνύματα, τα οποία συνήθως έχουν κακόβουλη πρόθεση, όπως ηλεκτρονικό ψάρεμα ή κακόβουλο λογισμικό, και τα μαζικά ανεπιθύμητα μηνύματα, τα οποία στοχεύουν να διαταράξουν την παραγωγικότητα ενός οργανισμού κατακλύζοντας το σύστημα ηλεκτρονικού ταχυδρομείου του (Mimecast, 2023).

Spoofing: Η πλαστογράφηση είναι μια άλλη απειλή ηλεκτρονικού ταχυδρομείου που περιλαμβάνει τον εισβολέα να πλαστοπροσωπεί μια αξιόπιστη οντότητα, είτε ένα άτομο είτε έναν οργανισμό, για να εξαπατήσει τον παραλήπτη. Η πλαστογράφηση παρουσιάζει δύο κύριες απειλές για τους οργανισμούς. Το πρώτο είναι η πλαστογράφηση ονομάτων τομέα, κατά την οποία ο εισβολέας πλαστογραφεί το όνομα τομέα ενός οργανισμού για να μιμηθεί τον οργανισμό και να εξαπατήσει ανυποψίαστα άτομα να πιστέψουν ότι το email είναι νόμιμο. Αυτό το είδος επίθεσης μπορεί να βλάψει τη φήμη ενός οργανισμού, ειδικά εάν τα

θύματα είναι πελάτες, όπως στην περίπτωση μιας τράπεζας. Η δεύτερη και πιο σημαντική απειλή είναι όταν οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν πλαστά email για να στοχεύσουν τους υπαλλήλους ενός οργανισμού και να αποκτήσουν πρόσβαση σε κρίσιμες πληροφορίες για περαιτέρω διείσδυση στα συστήματα του οργανισμού. Η πλαστογράφηση μπορεί να είναι ιδιαίτερα επικίνδυνη όταν συνδυάζεται με ηλεκτρονικό ψάρεμα, καθώς η διάκριση ανάμεσα σε ένα γνήσιο και ένα ψεύτικο email γίνεται όλο και πιο δύσκολη (Mimecast, 2023).

Business Email Compromise (BEC): Το BEC είναι μια απάτη κοινωνικής μηχανικής που στοχεύει σε προσωπικό υψηλού επιπέδου σε έναν οργανισμό. Οι εγκληματίες του κυβερνοχώρου προσπαθούν να αποκτήσουν πρόσβαση στον λογαριασμό email ενός στελέχους και στη συνέχεια χρησιμοποιούν την αναφορά για να κατευθύνουν υπαλλήλους σε λογιστικούς ή χρηματοοικονομικούς ρόλους για να μεταφέρουν χρήματα σε έναν λογαριασμό που ελέγχεται από τον εισβολέα. Αυτές οι επιθέσεις μπορούν επίσης να κλέψουν εταιρικά μυστικά (Mimecast, 2023).

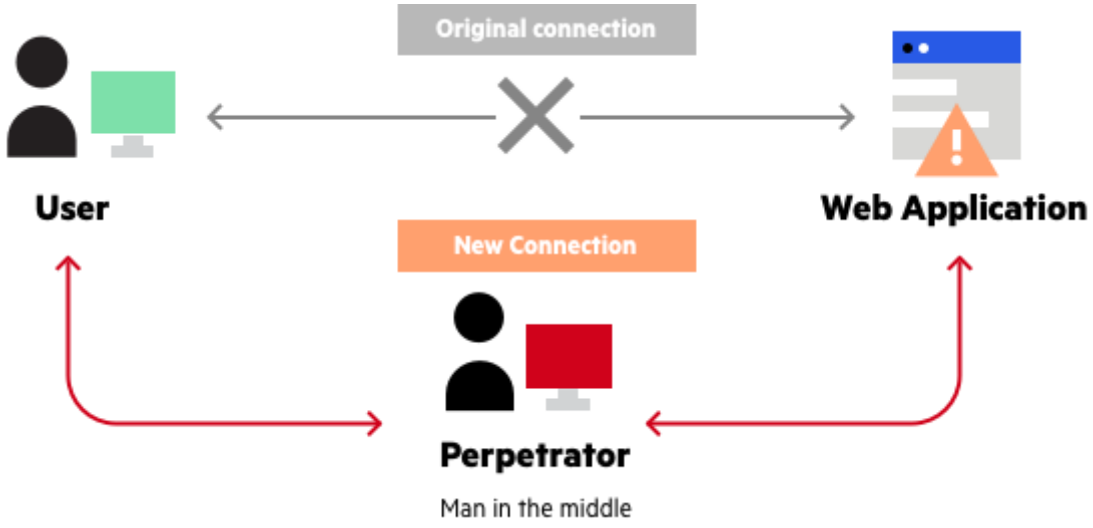
Παρά τις σημαντικές επενδύσεις στην εκπαίδευση και την τεχνολογία των εργαζομένων και των πελατών, οι απειλές μέσω email παραμένουν πρωταρχικό μέλημα για τους οργανισμούς και πρέπει συνεχώς να προσαρμόζουν τις άμυνές τους για να μετριάζουν αυτούς τους κινδύνους.

2.5 Threats Against Confidentiality

Αυτή η κατηγορία περιλαμβάνει περιπτώσεις παραβιάσεων ή διαρροών δεδομένων που μπορεί να βλάψουν το απόρρητο ενός οργανισμού. Σε τέτοιες περιπτώσεις, εμπιστευτικά ή προστατευμένα δεδομένα διαρρέουν σε ένα μη ασφαλές και αναξιόπιστο περιβάλλον. Παραβιάσεις δεδομένων μπορεί να προκύψουν μέσω επιθέσεων στον κυβερνοχώρο, εσωτερικών απειλών, καθώς και τυχαίας απώλειας ή έκθεσης δεδομένων. Ο κίνδυνος είναι σημαντικός δεδομένου ότι η πρόσβαση σε προστατευμένα δεδομένα είναι πρωταρχικός στόχος κακόβουλων οντοτήτων για διάφορους λόγους, όπως εκβιασμός, δυσφήμιση, παραπληροφόρηση και βιομηχανική κατασκοπεία.

Ίσως ο πιο γνωστός τύπος τέτοιας επίθεσης είναι η λεγόμενη επίθεση Man-in-the-Middle (MITM) (ENISA, 2021). Σε αυτήν την επίθεση, η κακόβουλη οντότητα εισέρχεται σε ανταλλαγή πληροφοριών μεταξύ δύο ανυποψίαστων οντοτήτων. Αφού αναχαιτίσει τη ροή δεδομένων, μπορεί να φιλτράρει, να κλέψει ή ακόμα και να τροποποιήσει μερικά από αυτά. Αυτές οι επιθέσεις πραγματοποιούνται πιο εύκολα όταν ένας επισκέπτης χρησιμοποιεί ένα κοινόχρηστο δίκτυο, όπως ένα δίκτυο WiFi σε δημόσιο χώρο, καθώς αυτά τα δίκτυα δεν προστατεύονται με κωδικό ασφαλείας.

Εικόνα 3. Εικονική αναπαράσταση μιας Man-in-the-Middle επίθεσης, April 21, 2023, <https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/>

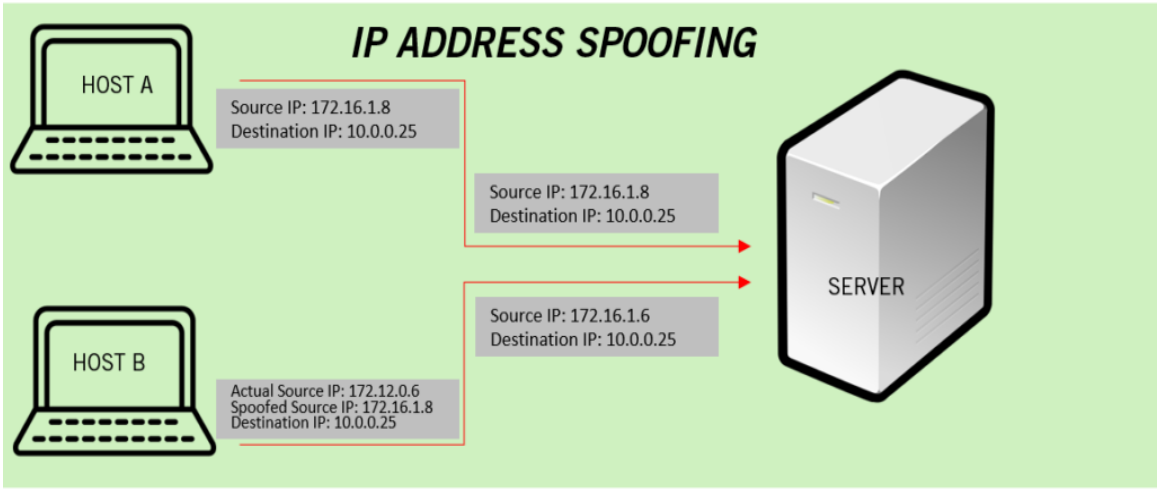


Μια επιτυχημένη επίθεση MITM αποτελείται από δύο φάσεις: υποκλοπή και αποκρυπτογράφηση. Η πρώτη φάση είναι η παρακολούθηση και η ανακατεύθυνση της ροής δεδομένων μέσα σε ένα δίκτυο πριν φτάσει στον προορισμό του. Ο πιο συνηθισμένος τρόπος είναι μέσω μιας παθητικής επίθεσης κατά την οποία ο εισβολέας δημιουργεί ένα δωρεάν κακόβουλο σημείο πρόσβασης Wi-Fi. Αυτά τα hotspot συνήθως ονομάζονται για να ταιριάζουν με την τοποθεσία τους και δεν προστατεύονται από κωδικό. Όταν το θύμα συνδέεται στο hotspot, ο εισβολέας έχει πλήρη ορατότητα σε όλες τις διαδικτυακές ανταλλαγές δεδομένων και μπορεί ελεύθερα να αναζητήσει ευαίσθητες πληροφορίες για κλοπή (Learning Center, 2019).

Εάν ένας εισβολέας επιθυμεί να λάβει μια πιο ενεργή στάση σε αυτή τη φάση, μπορεί να εκτελέσει μία από τις ακόλουθες επιθέσεις:

- ***IP spoofing***: Ο εισβολέας μεταμφιέζεται σε εφαρμογή αλλάζοντας τις κεφαλίδες των πακέτων σε μια διεύθυνση IP. Ως αποτέλεσμα, οι χρήστες που επιχειρούν να συνδεθούν σε μια συγκεκριμένη διεύθυνση URL σχετίζονται με την εφαρμογή και αποστέλλονται στη σελίδα του εισβολέα (Learning Center, 2019).

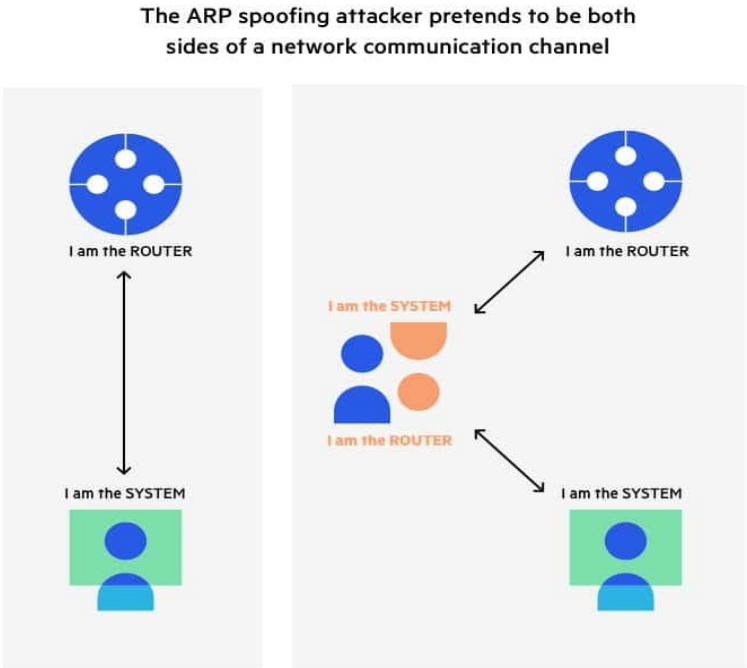
Εικόνα 4. Εικονική αναπαράσταση μιας IP Spoofing επίθεσης, 4 Δεκεμβρίου 2022, https://www.preveil.com/blog/man-in-the-middle-mitm-attacks/#:~:text=How%20MITM%20attacks%20intercept%20traffic,the%20wrong%20return%20address%20listed.



- ***ARP spoofing***: ARP spoofing είναι μια είδους επίθεσης στο δίκτυο, κατά την οποία ο επιτιθέμενος στέλνει ψεύτικα μηνύματα ARP (Adress Resolution Protocol) στο τοπικό δίκτυο. Το πρωτόκολλο ARP είναι υπεύθυνο για την αντιστοίχιση της IP διεύθυνσης ενός δικτύου σε σχέση με την αντίστοιχη MAC διεύθυνση του hardware. Στην επίθεση ARP spoofing, ο επιτιθέμενος συνδέει τη διεύθυνση IP του θύματος με τη δικιά του MAC διεύθυνση, επιτρέποντάς του να λαμβάνει όλα τα δεδομένα που προορίζονται για αυτή τη διεύθυνση IP (Address resolution protocol (ARP), 2023). Αυτό μπορεί να οδηγήσει σε διάφορες επιθέσεις, όπως παρακολούθηση ή υποκλοπή πληροφοριών. Η επίθεση ARP spoofing αποτελεί ένα σοβαρό πρόβλημα ασφαλείας δικτύου και πρέπει να αντιμετωπίζεται με κατάλληλα μέτρα πρόληψης και προστασίας (Learning Center, 2019).

Εικόνα 5. Εικονική αναπαράσταση μιας ARP Spoofing επίθεσης, April 21, 2023,

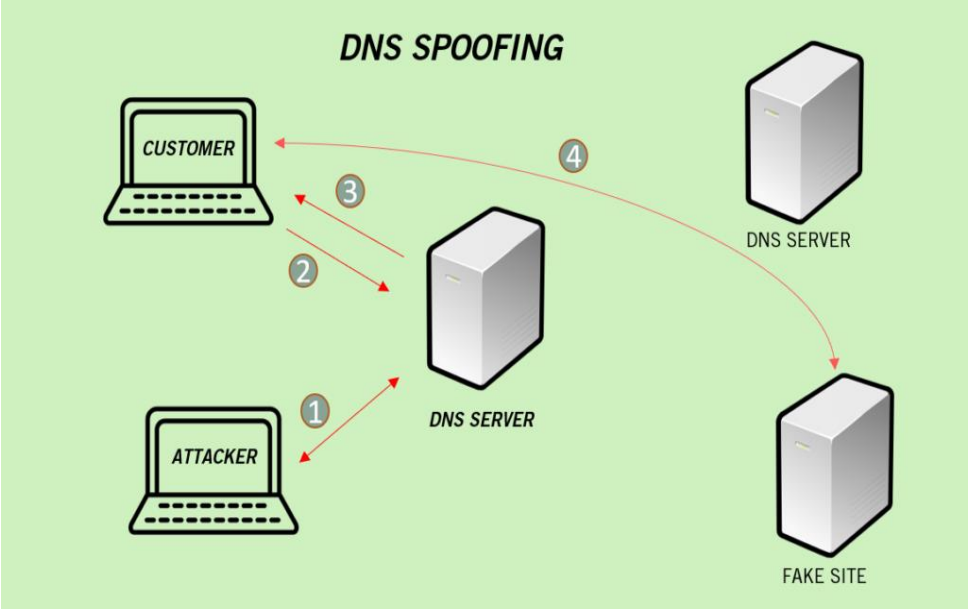
https://www.imperva.com/learn/application-security/arp-spoofing/



- ***DNS spoofing:*** Η πλαστογράφηση DNS, γνωστή και ως δηλητηρίαση κρυφής μνήμης DNS, περιλαμβάνει την κρυφή πρόσβαση σε έναν διακομιστή DNS για την αλλαγή του βιβλίου διευθύνσεων στον υπολογιστή του χρήστη. Ως αποτέλεσμα, οι χρήστες που επιχειρούν να αποκτήσουν πρόσβαση σε έναν ιστότοπο ανακατευθύνονται στη σελίδα του εισβολέα (Learning Center, 2019).

Εικόνα 6. Αναπαράσταση μιας DNS Spoofing επίθεσης, April 21, 2023,

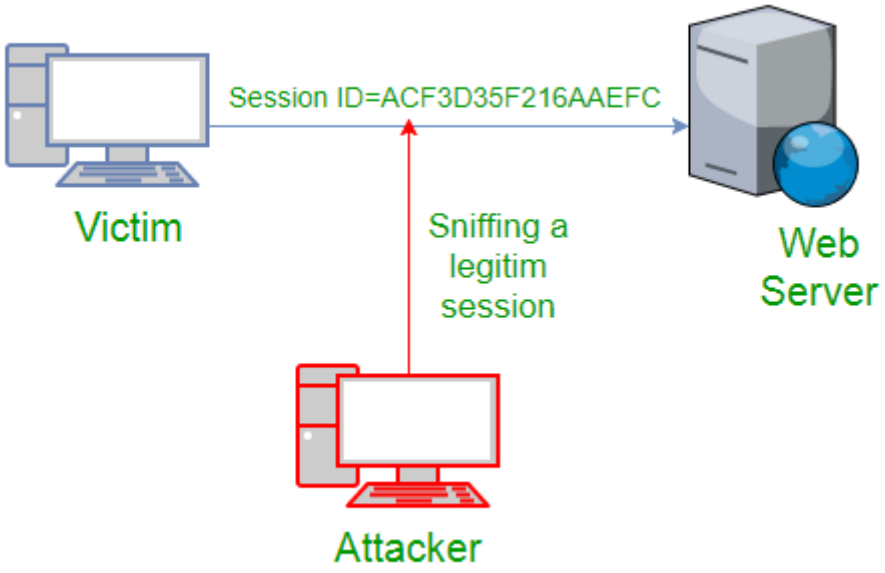
https://www.preveil.com/blog/man-in-the-middle-mitm-attacks/#:~:text=How%20MITM%20attacks%20intercept%20traffic,the%20wrong%20return%20address%20listed.



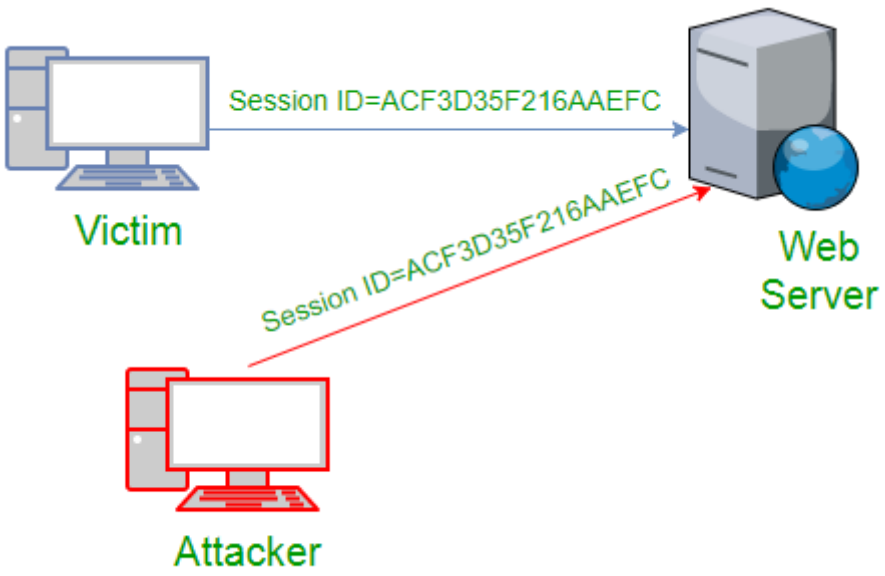
Session Spoofing: Το Session Spoofing, επίσης γνωστό ως Session Hijacking, είναι μια μέθοδος κατά την οποία ένας εισβολέας αποκτά τον έλεγχο μιας περιόδου σύνδεσης ιστού από έναν χρήστη. Μια συνεδρία είναι μια σειρά αλληλεπιδράσεων μεταξύ δύο οντοτήτων που επικοινωνούν κατά τη διάρκεια μιας σύνδεσης. Στοχεύει στη δημιουργία ενός «καναλιού» επικοινωνίας μεταξύ τους ώστε να μην απαιτείται έλεγχος ταυτότητας για κάθε ανταλλαγή δεδομένων. Κάθε περίοδος λειτουργίας έχει ένα User ID που επιτρέπει στο χρήστη να λαμβάνει δεδομένα ή να εκτελεί ενέργειες μέσα σε μια σύνδεση. Εάν ο εισβολέας

αποκτήσει αυτό το κλειδί, μπορεί να μιμηθεί τον χρήστη, να εκτελέσει τις ίδιες δραστηριότητες ή να αποδεχτεί τα ίδια δεδομένα (Learning Center, 2019).

Εικόνα 7. Εικονική αναπαράσταση μιας Session Spoofing επίθεσης , April 21, 20232022,https://www.geeksforgeeks.org/session-hijacking/



Εικόνα 8. Εικονική αναπαράσταση μιας Session Spoofing επίθεσης 2 , April 21, 2023, https://www.geeksforgeeks.org/session-hijacking/



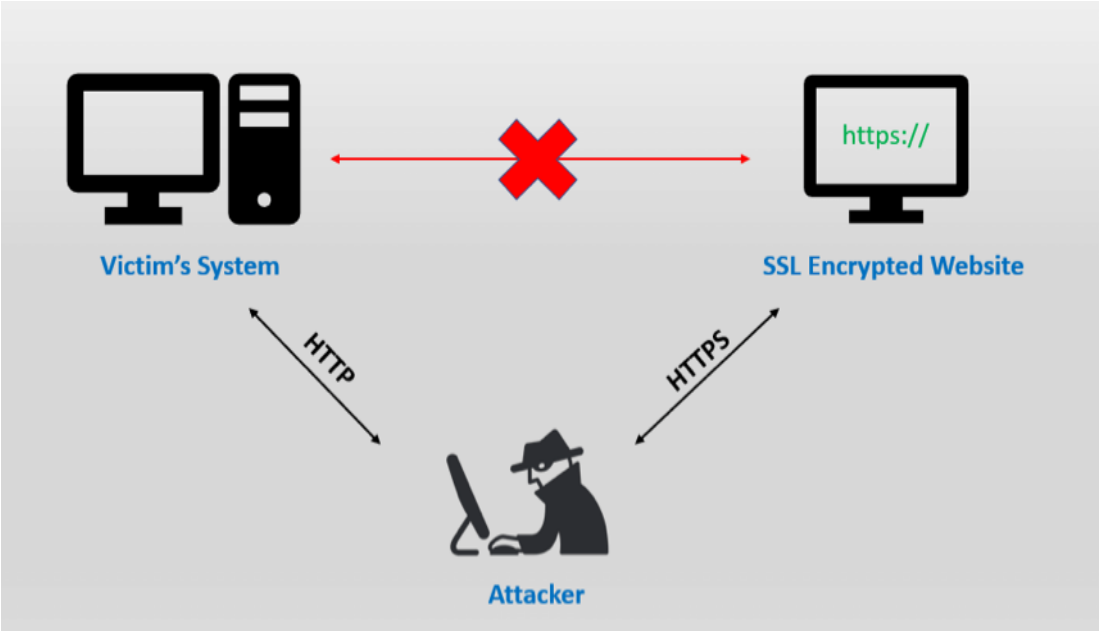
Μετά τη διαδικασία της υποκλοπής, η κρυπτογράφηση που προστατεύει τα αρχεία πρέπει να αποκρυπτογραφηθεί χωρίς να ειδοποιηθεί το θύμα (F5, 2023). Η κρυπτογράφηση

βασίζεται στο πρωτόκολλο SSL, ένα τεχνολογικό πρότυπο για την προστασία της ακεραιότητας των δεδομένων και την αναγνώριση οντοτήτων στο Διαδίκτυο. Χρησιμοποιεί ασύμμετρη κρυπτογραφία για την επίτευξη ασφαλούς σύνδεσης και συμμετρική κρυπτογραφία για ανταλλαγή δεδομένων. Ο έλεγχος ταυτότητας γίνεται μέσω ψηφιακών πιστοποιητικών SSL/TLS.

Υπάρχουν διάφορες μέθοδοι που χρησιμοποιούνται για την επίτευξη πλαστογράφησης συνεδριών, όπως:

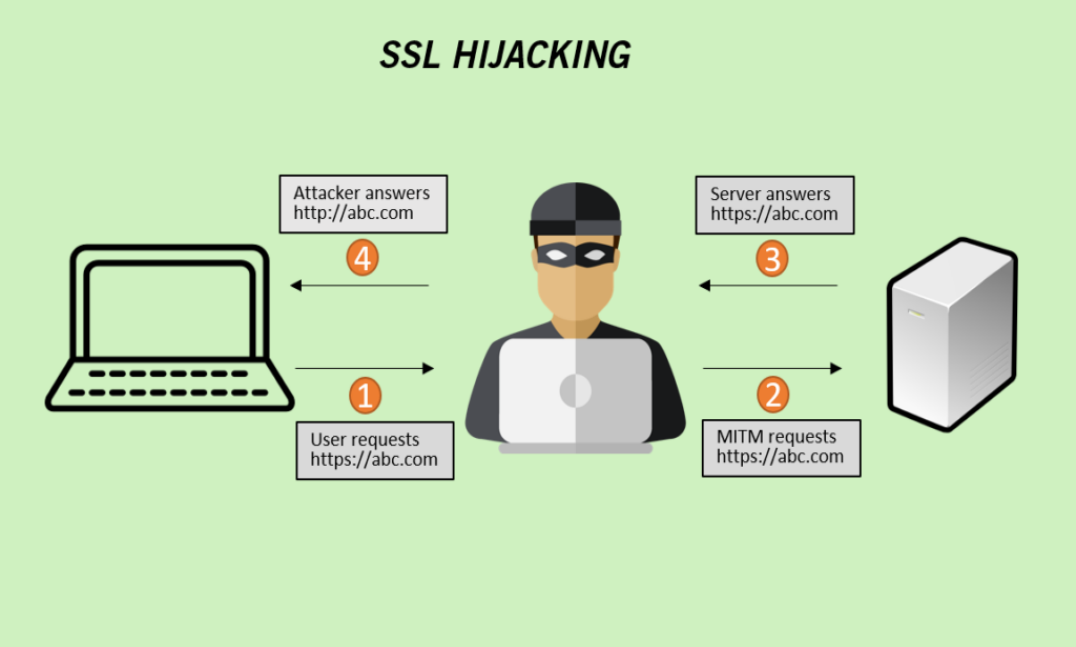
- ***Spoofing HTTPS***: Σε αυτήν την επίθεση, ο εισβολέας χρησιμοποιεί έναν τομέα που φαίνεται να είναι ο ιστότοπος-στόχος. Για να ενισχύσει την αξιοπιστία της απάτης, ο εισβολέας εγκαθιστά το πιστοποιητικό SSL του ιστότοπου-στόχου, κάνοντάς το να φαίνεται αυθεντικό και ασφαλές. Ο εισβολέας στέλνει στο θύμα έναν σύνδεσμο προς τον ψεύτικο ιστότοπο, ο οποίος μοιάζει με τον πραγματικό ιστότοπο, αλλά με χαρακτήρες που αντικαθίστανται από άλλους που είναι οπτικά παρόμοιοι. Για παράδειγμα, ο εισβολέας μπορεί να στείλει έναν σύνδεσμο στον ιστότοπο της Apple ως https://www.apple.com, αλλά με το αγγλικό "a" να αντικατασταθεί από το κυριλλικό "a" που μοιάζει πανομοιότυπο (Learning Center, 2019).
- ***SSL BEAST (Browser Exploit Against SSL/TLS)***: Στοχεύει σε μια ευπάθεια στην έκδοση 1.0 SSL/TLS. Εδώ, ο υπολογιστής του θύματος έχει μολυνθεί με κακόβουλο JavaScript που παρεμποδίζει τα κρυπτογραφημένα cookies που αποστέλλονται από μια εφαρμογή Ιστού. Στη συνέχεια, η αλυσίδα μπλοκ κρυπτογράφησης (CBC) μιας εφαρμογής παραβιάζεται για την αποκωδικοποίηση των cookie και των διακριτικών ελέγχου ταυτότητας (Learning Center, 2019).
- ***SSL Stripping***: Υποβαθμίζει μια σύνδεση HTTPS σε HTTP παρεμποδίζοντας τον έλεγχο ταυτότητας TLS που αποστέλλεται από μια εφαρμογή στον χρήστη. Ο εισβολέας στέλνει μια μη κρυπτογραφημένη έκδοση της σελίδας της εφαρμογής στον χρήστη, ενώ διατηρεί ασφαλή σύνδεση με την εφαρμογή. Εν τω μεταξύ, όλες οι ενέργειες του χρήστη στην εφαρμογή είναι ορατές στον εισβολέα (Learning Center, 2019).

Εικόνα 9. Εικονική αναπαράσταση μιας SSL Stripping διαδικασίας, April 21, 2023, https://www.venafi.com/blog/what-are-ssl-stripping-attacks



- ***SSL Hijacking***: Η SSL Hijacking, γνωστή και ως απογύμνωση SSL, είναι ένας τύπος επίθεσης στην οποία ένας εισβολέας παρέχει πλαστά κλειδιά ελέγχου ταυτότητας τόσο στον χρήστη όσο και στον ιστότοπο κατά τη διάρκεια μιας χειραψίας TCP. Αυτό επιτρέπει τη δημιουργία μιας φαινομενικά ασφαλούς σύνδεσης υπό τον έλεγχο του εισβολέα. Στο SSL Hijacking, ο εισβολέας παρεμποδίζει την κίνηση SSL μεταξύ του χρήστη και του διακομιστή web, την τροποποιεί και στη συνέχεια την προωθεί στον παραλήπτη χωρίς να εντοπιστεί. Αυτό επιτρέπει στον εισβολέα να αποκρυπτογραφεί, να παρακολουθεί και να χειρίζεται την κίνηση μεταξύ των δύο μερών χωρίς εντοπισμό. Η κλοπή SSL είναι μια σοβαρή απειλή, καθώς μπορεί να οδηγήσει σε κλοπή ευαίσθητων πληροφοριών, συμπεριλαμβανομένων κωδικών πρόσβασης, αριθμών πιστωτικών καρτών και άλλων προσωπικών δεδομένων (Learning Center, 2019).

Εικόνα 10. Εικονική αναπαράσταση μιας SSL Hijacking διαδικασίας, April 21, 2023, https://www.preveil.com/blog/man-in-the-middle-mitm-attacks/#:~:text=How%20MITM%20attacks%20intercept%20traffic,the%20wrong%20return%20address%20listed



Μια παραλλαγή της επίθεσης MiTM είναι η επίθεση Man on the Side. Σε αντίθεση με το MiTM, όπου ο εισβολέας αναλαμβάνει τον πλήρη έλεγχο ενός κόμβου, στην επίθεση στο πλάι, ο εισβολέας έχει απλώς πρόσβαση σε ένα κανάλι επικοινωνίας. Αυτό τους επιτρέπει να διαβάζουν τα δεδομένα που ανταλλάσσονται και να εισάγουν νέα δεδομένα. Ωστόσο, δεν τους επιτρέπει να τροποποιήσουν τα δεδομένα.

Ένας άλλος τύπος επίθεσης που έχει γίνει όλο και πιο δημοφιλής τα τελευταία χρόνια είναι οι επιθέσεις με αλυσίδα εφοδιασμού. Αυτές οι επιθέσεις είναι ικανές να προκαλέσουν καταστροφικές ζημιές εάν τους δοθεί αρκετός χρόνος. Στοχεύουν σε πωλητές και προμηθευτές και όχι σε μια συγκεκριμένη επιχείρηση, καθιστώντας πιο δύσκολο τον εντοπισμό και την αποτροπή τους εάν οι συνεργαζόμενες επιχειρήσεις δεν τηρούν αυστηρές πολιτικές ασφάλειας στον κυβερνοχώρο και χρησιμοποιούν τα καλύτερα εργαλεία (Password Manager & Digital Vault, 2023).

Μια επίθεση αλυσίδας εφοδιασμού συμβαίνει όταν ένας εισβολέας αποκτά πρόσβαση στο δίκτυο μιας επιχείρησης μέσω μιας συνεργαζόμενης επιχείρησης. Οι αλυσίδες ανεφοδιασμού μπορεί να είναι τεράστιες σε μέγεθος και πολύπλοκες στις σχέσεις τους, γεγονός που καθιστά δύσκολο τον εντοπισμό του αρχικού σημείου εισόδου σε ορισμένες επιθέσεις.

Οι επιθέσεις γνωστές ως «επιθέσεις εφοδιαστικής αλυσίδας» παρουσιάζονται σε διάφορες μορφές, με τις κυριότερες να είναι:

- ***Software Supply Chain Attack***: Αυτή η επίθεση απαιτεί μόνο ένα παραβιασμένο κομμάτι λογισμικού για την παράδοση κακόβουλου λογισμικού σε μια ολόκληρη αλυσίδα. Οι εισβολείς συχνά στοχεύουν τον πηγαίο κώδικα του λογισμικού, ενσωματώνοντας κακόβουλο κώδικα σε αξιόπιστο λογισμικό. Οι εισβολείς χρησιμοποιούν συχνά αναβαθμίσεις λογισμικού ως σημείο πρόσβασης. Το πρόβλημα με αυτές τις επιθέσεις είναι η δυσκολία στον εντοπισμό τους, καθώς οι εισβολείς χρησιμοποιούν κλεμμένα πιστοποιητικά για να «υπογράψουν» τον κώδικα, κάνοντάς τον να φαίνεται νόμιμος. Μια πρόσφατη επίθεση αυτού του είδους σημειώθηκε το 2020 στον λογαριασμό Orion της Solarwinds (Williams, 2020· Password Manager & Digital Vault, 2023).
- ***Hardware Supply Chain Attack***: Αυτές οι επιθέσεις χρησιμοποιούν φυσικές συσκευές. Στοχεύουν συσκευές που θα περάσουν από ολόκληρη την αλυσίδα, μεγιστοποιώντας την ακτίνα δράσης και τη ζημιά της επίθεσης. Για παράδειγμα, μπορεί να χρησιμοποιηθεί μια συσκευή USB ενσωματωμένη με keylogger, η οποία εγκαθίσταται από υπολογιστή σε υπολογιστή, καθώς ανυποψίαστα θύματα χρησιμοποιούν τη συσκευή για να μεταφέρουν δεδομένα (Password Manager & Digital Vault, 2023).
- ***Firmware Supply Chain Attack***: Εδώ, οι εισβολείς εισάγουν κακόβουλο λογισμικό στον κώδικα εκκίνησης ενός υπολογιστή. Αυτού του είδους οι επιθέσεις χρειάζονται δευτερόλεπτα για να πραγματοποιηθούν. Το κακόβουλο λογισμικό εκτελείται κατά την εκκίνηση του υπολογιστή, θέτοντας σε κίνδυνο ολόκληρο το σύστημα. Οι επιθέσεις υλικολογισμικού είναι γρήγορες και συχνά μη ανιχνεύσιμες εάν κάποιος δεν αναζητά μια τέτοια επίθεση (Password Manager & Digital Vault, 2023).

2.6 Threats Against Availability and Integrity

Η προσβασιμότητα και η ακεραιότητα είναι στόχοι μιας πληθώρας επιθέσεων. Δύο ξεχωριστές ομάδες επιθέσεων που ξεχωρίζουν είναι το Denial of Service (DoS) και το SQL Injection. Το DoS είναι μια από τις πιο σημαντικές επιθέσεις στα πληροφοριακά συστήματα, καθώς στοχεύει την προσβασιμότητα ενός συστήματος εξαντλώντας τους πόρους επεξεργασίας του, προκαλώντας μειωμένη απόδοση, απώλεια δεδομένων και περιόδους μη διαθεσιμότητας μιας υπηρεσίας. Αυτή η απειλή θεωρείται αρκετά υψηλή λόγω της συχνής εμφάνισής της σε πραγματικά γεγονότα καθώς και της δυνητικά σημαντικής επίδρασής της. Εξίσου σημαντική είναι η επίθεση SQL Injection, ένας τύπος κυβερνοεπίθεσης που επιτυγχάνεται με την έγχυση κακόβουλου κώδικα σε έναν SQL Server, μέσω του οποίου ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στα περιεχόμενα μιας βάσης δεδομένων (ENISA, 2021).

2.6.1 Denial of Service

Οι επιθέσεις Distributed Denial of Service (DDoS) αναφέρονται συχνά ως επιθέσεις δικτύου που εκμεταλλεύονται τα πεπερασμένα όρια των πόρων ενός δικτύου και την υποδομή που υποστηρίζει τον ιστότοπο μιας εταιρείας. Αυτοί οι τύποι επιθέσεων περιλαμβάνουν την αποστολή πολλαπλών πακέτων ερωτημάτων στον στοχευμένο ιστότοπο για να υπερβούν τον μέγιστο αριθμό ερωτημάτων που μπορεί να διαχειριστεί ο ιστότοπος, εμποδίζοντας έτσι την κανονική του λειτουργία (Kaspersky, 2023a). Το επίπεδο εξυπηρέτησης επηρεάζεται με τους εξής τρόπους:

- Η απάντηση σε ερωτήματα είναι πιο αργή από ό,τι συνήθως.
- Ορισμένα ή όλα τα ερωτήματα αγνοούνται.

Ο πρωταρχικός στόχος των επιθέσεων DDoS είναι συνήθως η πρόκληση ολικής διακοπής στις καθημερινές λειτουργίες ενός ιστότοπου, οδηγώντας σε γενική άρνηση παροχής υπηρεσιών. Οι επιθέσεις DDoS χρησιμοποιούνται για οικονομικό όφελος, για την απαξίωση μιας οντότητας ή για την πρόκληση ζημίας στις υπηρεσίες ενός ανταγωνιστή (Cloudflare, 2023). Ένα νέο στυλ επίθεσης είναι το Ransom Denial of Service (RDoS), το οποίο διατίθεται σε δύο παραλλαγές: μια επίθεση που ακολουθείται από μια απαίτηση λύτρων ή, πρώτα, μια απαίτηση λύτρων που συνοδεύεται από μια επίθεση μικρής κλίμακας. Στο πρώτο σενάριο,

πραγματοποιείται μια επίθεση και ζητούνται λύτρα για να τερματιστεί το ξόρκι. Στη δεύτερη, ζητείται λύτρα, μαζί με επίθεση μικρής κλίμακας, για να αποφευχθούν μελλοντικές κλιμακώσεις της επιθετικότητας.

Οι εισβολείς πρέπει να χρησιμοποιούν αυτοματοποιημένες μεθόδους για να στείλουν έναν τεράστιο όγκο ερωτημάτων στο θύμα, όπως ένα botnet υπολογιστών που έχουν μολυνθεί με κακόβουλο λογισμικό. Με αυτόν τον τρόπο, η κλίμακα της επίθεσης μπορεί να υπερβεί την ικανότητα διαχείρισης του συστήματος θύματος.

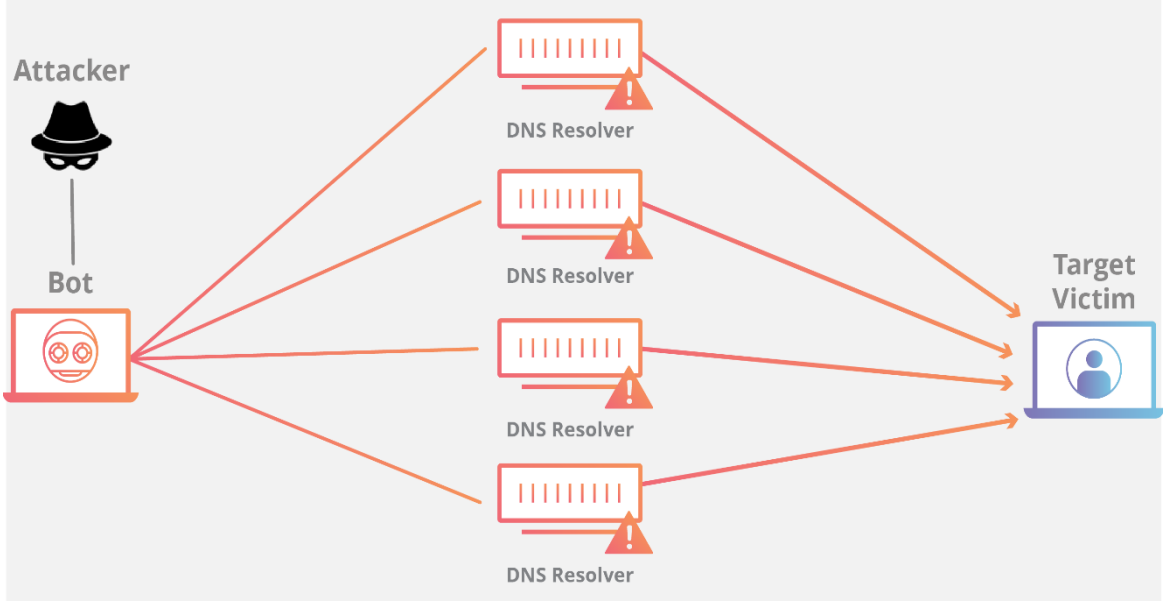
Η αποστολή μεγάλου όγκου ερωτημάτων στο θύμα είναι ένα εγγενές χαρακτηριστικό των επιθέσεων κατανεμημένης άρνησης υπηρεσίας (DDoS). Οι εισβολείς συνήθως χρησιμοποιούν αυτοματοποιημένες μεθόδους, όπως botnet που αποτελούνται από υπολογιστές που έχουν μολυνθεί από κακόβουλο λογισμικό, για να το επιτύχουν αυτό. Κατά συνέπεια, η κλίμακα μιας τέτοιας επίθεσης μπορεί να υπερβαίνει την ικανότητα του συστήματος στόχου να τη χειριστεί. Το πιο κοινό σύμπτωμα μιας επίθεσης DDoS σε έναν ιστότοπο είναι η σημαντική μείωση του χρόνου απόκρισης και της διαθεσιμότητας. Ωστόσο, υπάρχουν επίσης συχνές περιπτώσεις, όπως παροδικές αιχμές στην επισκεψιμότητα του ιστότοπου, που μπορεί να προκαλέσουν παρόμοια προβλήματα, αλλά είναι φυσιολογική δραστηριότητα του συστήματος και όχι αποτέλεσμα κακόβουλης ενέργειας. Ως εκ τούτου, απαιτείται περαιτέρω διερεύνηση, η οποία μπορεί να επιτευχθεί χρησιμοποιώντας εργαλεία ανάλυσης κυκλοφορίας που μπορούν να βοηθήσουν στον εντοπισμό δεικτών που σηματοδοτούν μια τέτοια επίθεση (Cloudflare, 2023a). Αυτοί οι δείκτες περιλαμβάνουν ύποπτο όγκο επισκεψιμότητας που προέρχεται από μια μεμονωμένη διεύθυνση IP ή εύρος IP, μεγάλο όγκο επισκεψιμότητας από χρήστες που μοιράζονται το ίδιο προφίλ, όπως τύπο συσκευής, γεωγραφική τοποθεσία, έκδοση προγράμματος περιήγησης και άλλα, μια σημαντική και ανεξήγητη αύξηση σε ερωτήματα από μία μόνο σελίδα και ασυνήθιστα μοτίβα κίνησης, όπως αιχμές κατά τις μονές ώρες της ημέρας.

Οι επιθέσεις DDoS μπορούν να χωριστούν σε τρεις κατηγορίες που στοχεύουν διαφορετικά μέρη ενός δικτύου (Learning Center, 2022):

- ***Volume Based Attacks***: Αυτή η κατηγορία περιλαμβάνει πλημμύρες UDP, πλημμύρες ICMP και άλλες πλημμύρες πλαστών πακέτων. Ο στόχος της επίθεσης είναι να

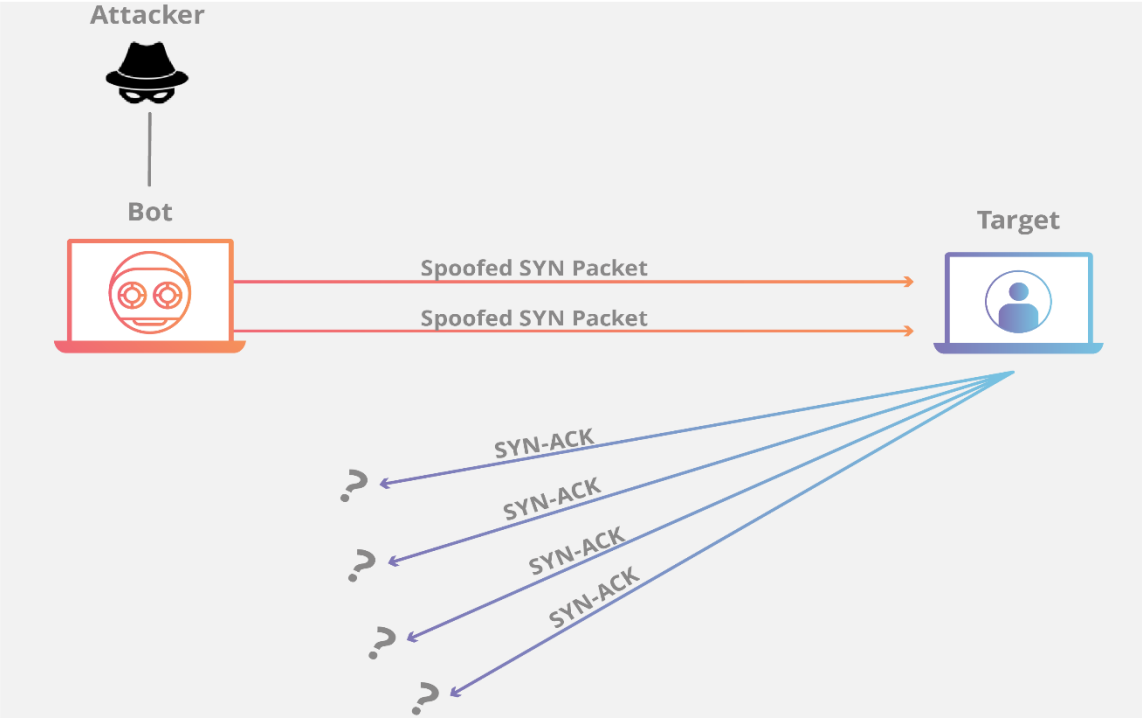
καταναλώσει το διαθέσιμο εύρος ζώνης της στοχευμένης σελίδας. Η έντασή του μετριέται σε bit ανά δευτερόλεπτο (Bps) (Learning Center, 2022).

Εικόνα 11. Εικονική αναπαράσταση μιας Volume Based Attack, April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/



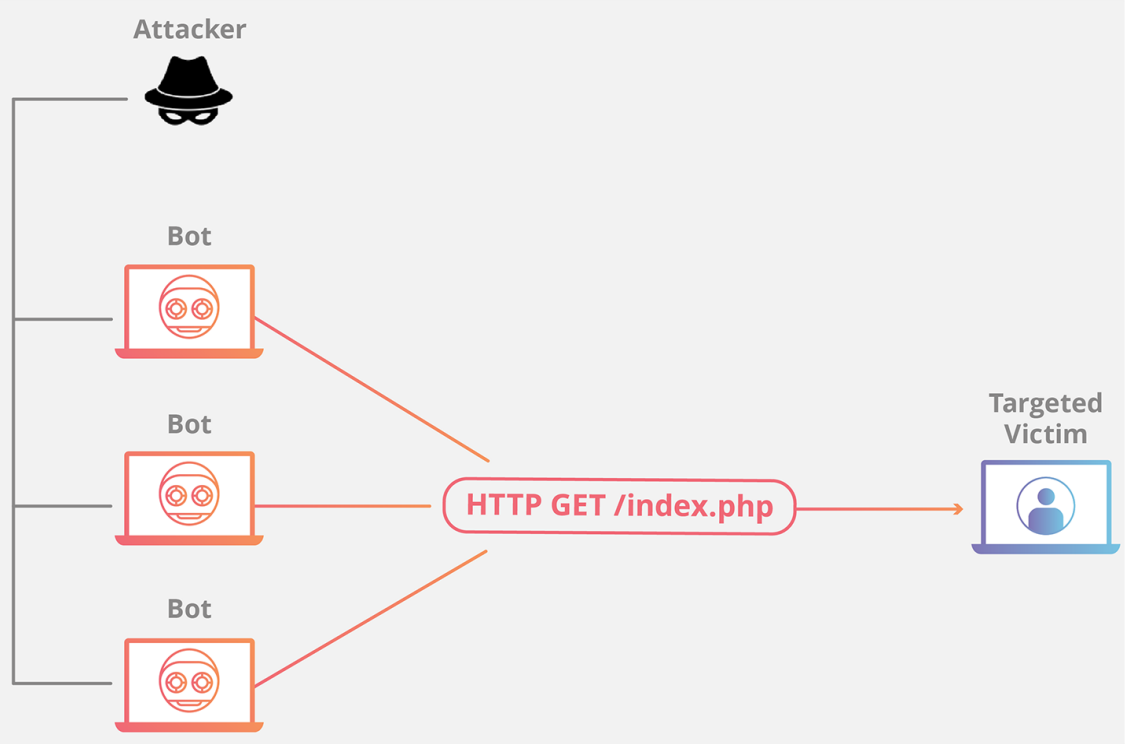
- ***Protocol Attacks***: αναφέρεται σε ένα είδος επιθέσεων DDoS, το οποίο περιλαμβάνει SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS και άλλα. Κατά τη διάρκεια αυτού του είδους επιθέσεων, οι επιτιθέμενοι καταναλώνουν πόρους από ενδιάμεσα συστήματα επικοινωνιών, όπως firewalls, load balancers και άλλα. Η ένταση της επίθεσης μετριέται σε packets per second (Pps) (Learning Center, 2022).

Εικόνα 12. Εικονική αναπαράσταση μιας Protocol επίθεσης , April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/



- ***Application Layer Attacks***: Οι επιθέσεις επιπέδου εφαρμογής είναι ένας τύπος επίθεσης DDoS που στοχεύει το επίπεδο εφαρμογής ενός δικτύου. Αυτές οι επιθέσεις περιλαμβάνουν χαμηλές και αργές επιθέσεις, πλημμύρες GET/POST, επιθέσεις που εκμεταλλεύονται τρωτά σημεία στον Apache ή στο λειτουργικό σύστημα και γενικές επιθέσεις που εστιάζουν στο επίπεδο εφαρμογής. Οι επιθέσεις επιπέδου εφαρμογής αποτελούνται από φαινομενικά νόμιμες και αθώες αιτήσεις, σκοπός των οποίων είναι η υπερφόρτωση του διακομιστή. Η ένταση αυτών των επιθέσεων μετριέται σε αιτήματα ανά δευτερόλεπτο (Rps) (Learning Center, 2022).

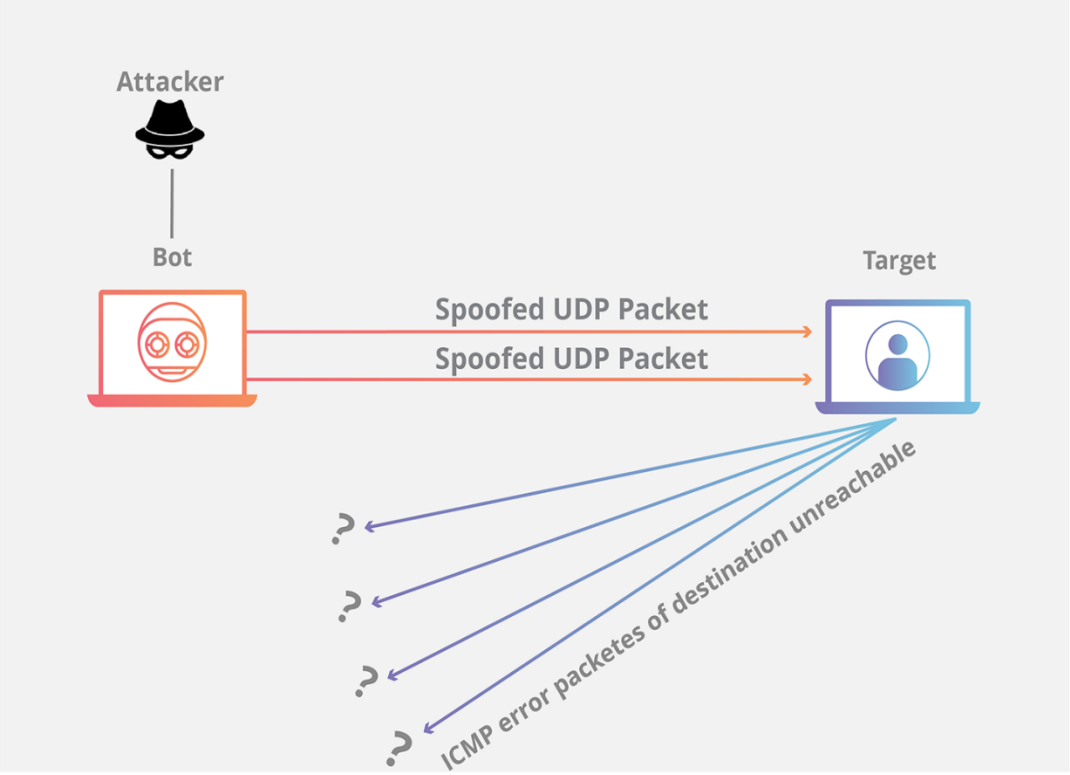
Εικόνα 13. Εικονική αναπαράσταση του Application Layer επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/



Όπως γίνεται φανερό, οι επιθέσεις DDoS αποτελούνται από ένα ευρύ φάσμα τεχνικών που χρησιμοποιούνται για τη στόχευση διαφορετικών σημείων συστήματος. Στη συνέχεια, ορισμένες κυρίαρχες μέθοδοι θα εξηγηθούν με περισσότερες λεπτομέρειες.

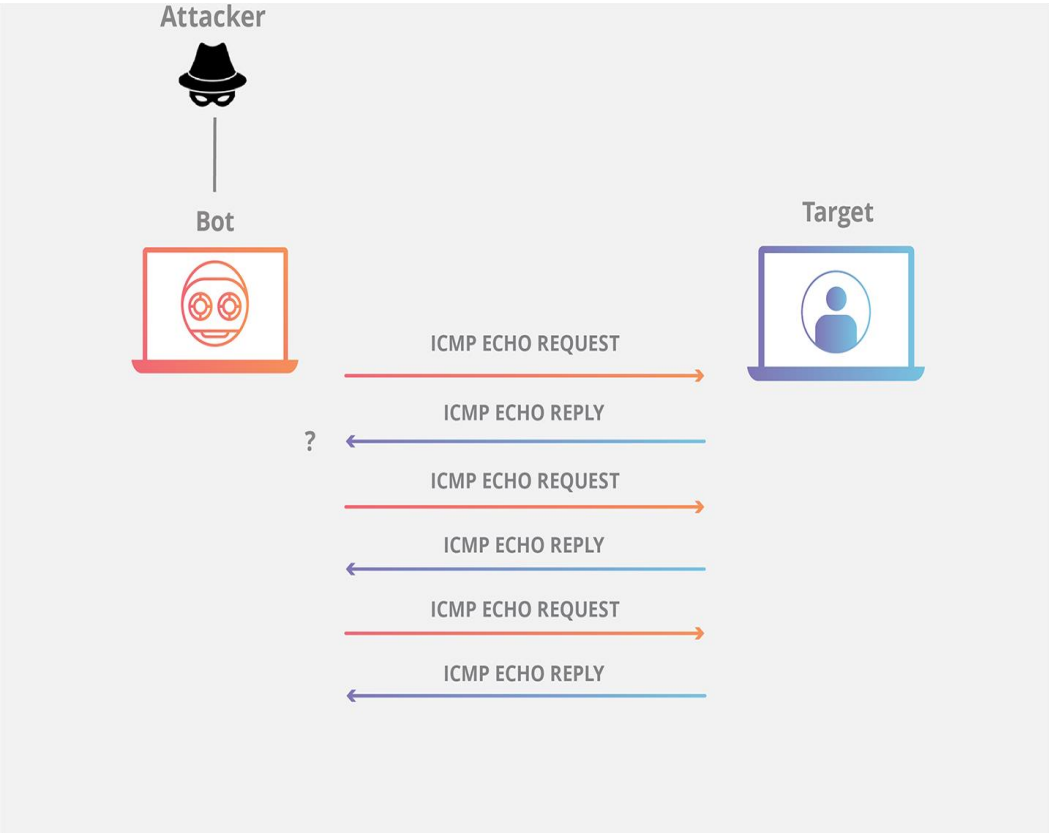
- ***UDP flood***: Μια επίθεση πλημμύρας UDP είναι οποιαδήποτε επίθεση DDoS που πλημμυρίζει τον στόχο με πακέτα User Datagram Protocol (UDP). Ο στόχος είναι να απορροφηθεί μια τυχαία θύρα του στοχευμένου διακομιστή. Αυτό αναγκάζει τον διακομιστή να ελέγχει επανειλημμένα εάν κάποια εφαρμογή επικοινωνεί με άλλη εφαρμογή σε αυτήν τη θύρα. Εάν δεν βρεθεί καμία εφαρμογή, απαντήστε με ένα πακέτο ICMP "Απρόσιτος προορισμός". Αυτό καταναλώνει σημαντικούς πόρους του κεντρικού υπολογιστή και μπορεί να οδηγήσει σε μη διαθεσιμότητα (Learning Center, 2022).

Εικόνα 14. Εικονική αναπαράσταση μιας UDP Flood επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/



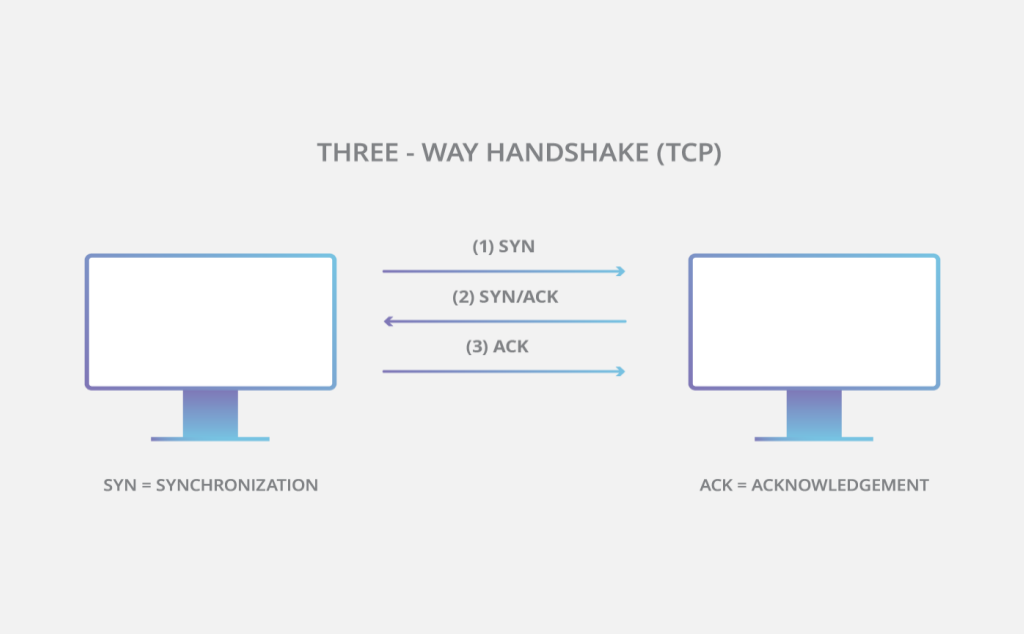
- ***ICMP (Ping) flood***: Το ICMP (Ping) flood είναι ένας τύπος επίθεσης DDoS που κατακλύζει τους πόρους του στόχου μέσω των πακέτων ICMP Echo Request (ping). Στέλνει συνεχώς πακέτα χωρίς να περιμένει απάντηση. Αυτός ο τύπος επίθεσης μπορεί να καταναλώσει εισερχόμενο και εξερχόμενο εύρος ζώνης, καθώς οι διακομιστές του θύματος θα προσπαθήσουν να ανταποκριθούν με πακέτα ICMP Echo Reply, οδηγώντας σε σημαντική μείωση στην απόδοση του συστήματος εάν ο αριθμός των πακέτων που πρέπει να εξυπηρετηθούν είναι πολύ μεγάλος (Learning Center, 2022).

Εικόνα 15. Εικονική αναπαράστασης μιας ICPM (Ping) Flood επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

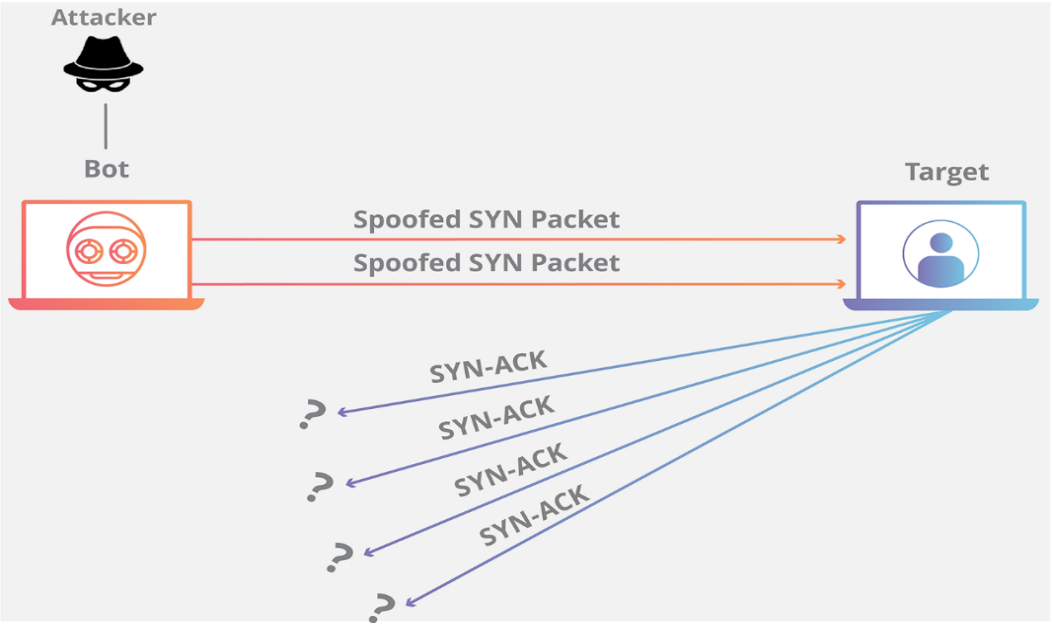


- ***SYN flood***: Μια επίθεση πλημμύρας SYN εκμεταλλεύεται μια γνωστή αδυναμία στην ακολουθία σύνδεσης TCP. Ένα πακέτο SYN (Συγχρονισμός) για την εκκίνηση μιας σύνδεσης TCP με έναν κεντρικό υπολογιστή πρέπει να απαντηθεί με ένα πακέτο SYN-ACK (Συγχρονισμός-Επιβεβαίωση) από τον κεντρικό υπολογιστή και να επαληθευτεί με ένα πακέτο ACK από τον αποστολέα. Σε ένα σενάριο πλημμύρας SYN, ο εισβολέας στέλνει πολλά πακέτα SYN αλλά είτε δεν ανταποκρίνεται στην απόκριση SYN-ACK του κεντρικού υπολογιστή είτε στέλνει αιτήματα SYN από μια πλαστογραφημένη διεύθυνση IP. Και στις δύο περιπτώσεις, το σύστημα συνεχίζει να περιμένει για επιβεβαίωση καθενός από αυτά τα αιτήματα, καταναλώνοντας πόρους μέχρι να φτάσει στο σημείο όπου δεν μπορεί να δημιουργήσει νέες συνδέσεις, με αποτέλεσμα την άρνηση της υπηρεσίας (Learning Center, 2022).

Εικόνα 16. Εικονική αναπαράσταση της διαδικασίας συγχρονισμού, April 21, 2023,https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

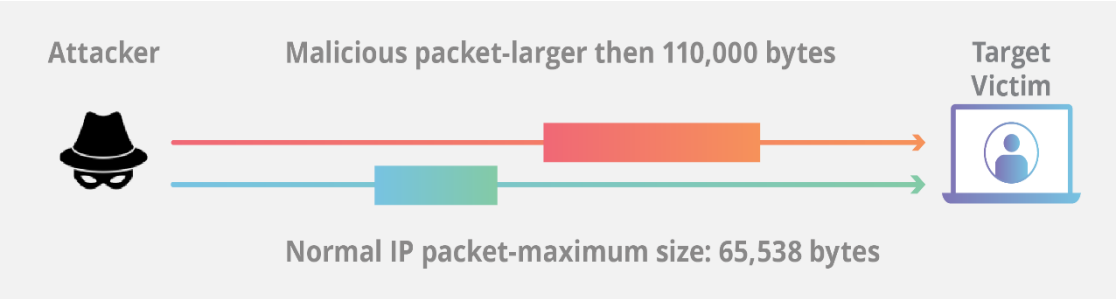


Εικόνα 17. Εικονική αναπαράσταση μιας SYN Flood επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/



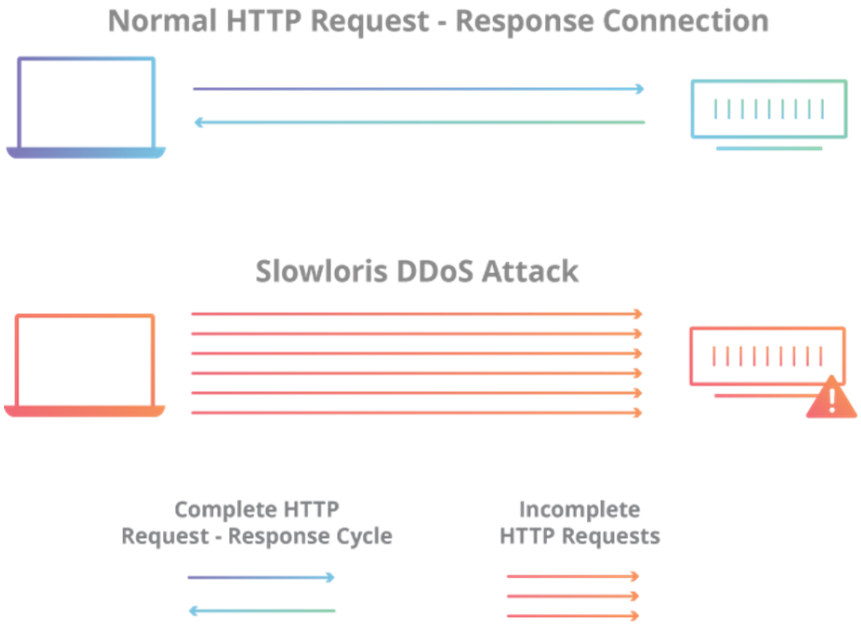
- ***Ping of Death:*** Σε μια επίθεση ping of death, ο εισβολέας στέλνει πολλαπλά κακόβουλα πακέτα ping σε ένα σύστημα. Το μέγιστο μέγεθος ενός πακέτου IP είναι 65.535 byte. Ωστόσο, το επίπεδο σύνδεσης δεδομένων συνήθως επιβάλλει όρια στο μέγιστο μέγεθος πλαισίου, το οποίο στο Ethernet είναι συνήθως 1500 byte. Σε αυτήν την περίπτωση, ένα πακέτο μεγάλου μεγέθους χωρίζεται σε πολλαπλά πακέτα IP και ο παραλήπτης συναρμολογεί εκ νέου αυτά τα κομμάτια σε ένα πλήρες πακέτο. Σε μια επίθεση ping-of-death, ο παραλήπτης λαμβάνει ένα τελικό πακέτο μεγαλύτερο από 65.535 byte. Αυτό μπορεί να προκαλέσει υπερχείλιση στη μνήμη που έχει εκχωρηθεί για πακέτα, προκαλώντας μη διαθεσιμότητα για την κανονική κυκλοφορία δικτύου (Learning Center, 2022).

Εικόνα 18. Εικονική αναπαράσταση μιας Ping of Death επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/ping-of-death-ddos-attack/



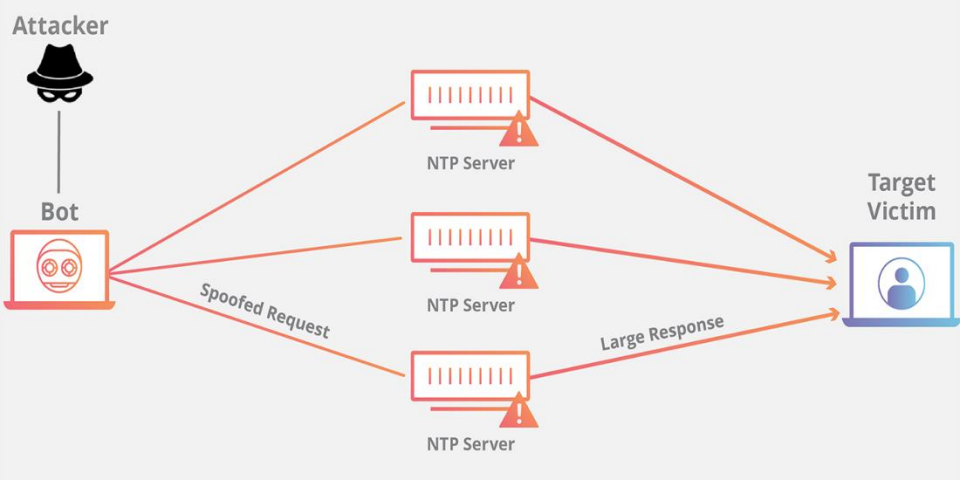
- ***Slowloris:*** Η επίθεση Slowloris αποτελεί μια μέθοδο επιτίθεσης που στοχεύει σε έναν web server και επιτρέπει στον επιτιθέμενο να «εξαντλήσει» το στόχο χωρίς να επηρεάσει άλλες υπηρεσίες στο δίκτυο. Η επίτευξη αυτού του στόχου γίνεται μέσω της διατήρησης όσο το δυνατόν περισσότερων ανοιχτών συνδέσεων με τον στόχο. Αυτό επιτυγχάνεται με τη δημιουργία συνδέσεων και την αποστολή μη ολοκληρωμένων επερωτήσεων. Ο στόχος κρατά κάθε μία από αυτές τις ψεύτικες συνδέσεις ανοιχτή, η οποία καταλήγει στον υπερβολικό αριθμό των ταυτόχρονων συνδέσεων και συνεπώς σε άρνηση υπηρεσίας για νέες έμπιστες συνδέσεις (Learning Center, 2022).

Εικόνα 19. Εικονική αναπαράσταση μιας Slowloris επίθεσης, April 21, 2023, https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/



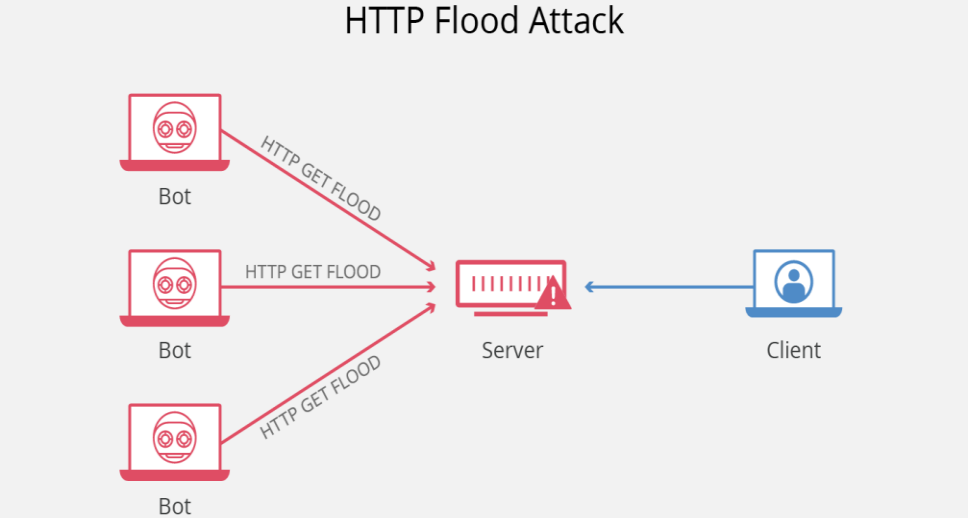
- ***NTP Amplification***: Σε μια επίθεση NTP Amplification, ένας εισβολέας εκμεταλλεύεται ελεύθερα προσβάσιμους διακομιστές Network Time Protocol (NTP) για να κατακλύσει τον στοχευμένο διακομιστή με κίνηση UDP. Το NTP είναι ένα πρωτόκολλο που χρησιμοποιείται για συγχρονισμό ρολογιού μεταξύ συστημάτων υπολογιστών. Ο εισβολέας χρησιμοποιεί ένα botnet για να στείλει πακέτα UDP με πλαστές διευθύνσεις IP σε έναν διακομιστή NTP που έχει ενεργοποιημένη μια συγκεκριμένη εντολή (monlist). Η επίθεση ονομάζεται επίθεση ενίσχυσης επειδή η αναλογία ερωτήματος προς απάντηση σε τέτοιες περιπτώσεις είναι κάπου μεταξύ 1:20 και 1:200 ή και περισσότερο. Αυτό σημαίνει ότι κάθε εισβολέας που λαμβάνει μια λίστα διακομιστών NTP μπορεί εύκολα να δημιουργήσει μια καταστροφική επίθεση DDoS μεγάλου εύρους ζώνης και μεγάλου όγκου (Learning Center, 2022).

Εικόνα 20. Εικονική αναπαράσταση μιας NTP Amplification επίθεσης , April 21, 2023, https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/



- ***HTTP Flood***: Σε μια επίθεση HTTP flood DDoS, ο εισβολέας εκμεταλλεύεται φαινομενικά νόμιμα αιτήματα HTTP GET ή POST για να επιτεθεί σε έναν διακομιστή. Οι πλημμύρες HTTP δεν χρησιμοποιούν κακόβουλα πακέτα, τεχνικές πλαστογράφησης ή ανάκλασης και απαιτούν μικρότερο εύρος ζώνης σε σύγκριση με άλλες επιθέσεις για την κατάρριψη ενός στόχου. Αυτή η επίθεση είναι πιο αποτελεσματική όταν αναγκάζει έναν διακομιστή να χρησιμοποιήσει τους μέγιστους δυνατούς πόρους για να απαντήσει σε κάθε αίτημα (Learning Center, 2022).

Εικόνα 21. Εικονική αναπαράσταση μιας HTTP επίθεσης , April 21, 2023, https://www.cloudflare.com/learning/ddos/http-flood-ddos-attack/



2.6.2 SQL Injection

Ο κώδικας SQL χρησιμοποιείται για τον χειρισμό μιας βάσης δεδομένων για πρόσβαση σε πληροφορίες που δεν είναι διαθέσιμες μέσω του στοχευμένου ιστότοπου. Αυτές οι πληροφορίες μπορεί να περιλαμβάνουν ευαίσθητα εταιρικά δεδομένα, λίστες χρηστών, λίστες πελατών και οποιοδήποτε αντικείμενο είναι αποθηκευμένο σε μια σχεσιακή βάση δεδομένων. Μπορεί ακόμη και να οδηγήσει στον εισβολέα να αποκτήσει δικαιώματα διαχειριστή στη βάση δεδομένων, επομένως οι πιθανές συνέπειες μιας επιτυχημένης επίθεσης μπορεί να είναι σημαντικές, ειδικά στον τομέα των προσωπικών δεδομένων και της πνευματικής ιδιοκτησίας (Learning Center, 2023a).

Συνήθως, οι επιθέσεις SQL injection ταξινομούνται σε τρεις κατηγορίες με βάση τη μέθοδο που χρησιμοποιούν για να αποκτήσουν πρόσβαση στα δεδομένα:

- In-band SQLi (Classic)
- Inferential SQLi (Blind)
- Out-of-band SQLI.

Στη συνέχεια, θα αναλύσουμε αυτές τις τρεις μεθόδους με περισσότερες λεπτομέρειες.

2.6.2.1 In-band SQLi

Ο εισβολέας χρησιμοποιεί την ίδια διεπαφή για να πραγματοποιήσει την επίθεση και να συλλέξει αποτελέσματα. Η απλότητα και η αποτελεσματικότητα του In-band SQLi το καθιστούν έναν από τους πιο συνηθισμένους τύπους. Υπάρχουν δύο υποτύποι αυτής της μεθόδου (Learning Center, 2023a):

- SQLi που βασίζεται σε σφάλματα: Ο εισβολέας εκτελεί ενέργειες που προκαλούν τη δημιουργία μηνυμάτων σφάλματος στη βάση δεδομένων. Τα μηνύματα που δημιουργούνται ενδέχεται να αποκαλύπτουν πληροφορίες σχετικά με τη δομή της βάσης δεδομένων.
- SQLi που βασίζεται σε ένωση: Αυτή η τεχνική εκμεταλλεύεται την εντολή UNION της SQL, η οποία επιστρέφει αποτελέσματα που είναι ένας συνδυασμός στηλών από πολλούς πίνακες σε μια απόκριση HTTP. Η απάντηση μπορεί να περιέχει δεδομένα που μπορούν να χρησιμοποιηθούν κακόβουλα από τον εισβολέα.

2.6.2.2 Inferential (Blind) SQLi

Ο εισβολέας στέλνει πακέτα δεδομένων στον διακομιστή και παρατηρεί την απόκριση και τη συμπεριφορά του για να μάθει περισσότερα για τη δομή της βάσης δεδομένων. Αυτή η μέθοδος ονομάζεται τυφλή επειδή τα δεδομένα δεν μεταφέρονται από τη βάση δεδομένων στον εισβολέα. Έτσι ο εισβολέας δεν μπορεί να δει τις πληροφορίες. Ο εισβολέας ανακατασκευάζει τη βάση δεδομένων στέλνοντας ερωτήματα, παρατηρώντας τις απαντήσεις και τη συμπεριφορά του διακομιστή.

Οι τυφλές επιθέσεις έγχυσης SQL μπορούν να κατηγοριοποιηθούν ως εξής (Learning Center, 2023a):

- ***Βασισμένο σε Boolean***: Ο εισβολέας στέλνει ένα ερώτημα SQL στη βάση δεδομένων, κάνοντας την εφαρμογή να επιστρέψει ένα αποτέλεσμα. Το αποτέλεσμα μπορεί να διαφέρει ανάλογα με το αν το ερώτημα είναι αληθές ή ψευδές. Με βάση την εξέλιξη, θα τροποποιηθούν οι πληροφορίες εντός της απόκρισης HTTP ή όχι. Έτσι, στέλνοντας πολλαπλές ερωτήσεις, ο εισβολέας μπορεί σταδιακά να συλλέγει πληροφορίες σχετικά με τη δομή και το περιεχόμενο της βάσης δεδομένων.
- ***Βάσει χρόνου***: Ο εισβολέας στέλνει ένα ερώτημα SQL στη βάση δεδομένων, το οποίο θα χρειαστεί λίγο χρόνο για να επεξεργαστεί το ερώτημα, να δημιουργήσει και να στείλει την απάντηση. Ο εισβολέας μπορεί να εκτιμήσει από τον χρόνο απόκρισης εάν το ερώτημα είναι αληθές ή ψευδές και να εξάγει πληροφορίες σχετικά με τη δομή της βάσης δεδομένων χωρίς να βασίζεται σε δεδομένα από τη βάση δεδομένων.

2.6.2.3 Out-of-Band SQLi

Το Out-of-band SQLi είναι μια επιθετική τεχνική που χρησιμοποιείται όταν ο επιτιθέμενος δεν μπορεί να χρησιμοποιήσει την ίδια διασύνδεση για να πραγματοποιήσει τις επιθέσεις του και να συλλέξει τα αποτελέσματα ή όταν ο διακομιστής είναι αργός ή ασταθής για να εκτελεστεί Inferential SQLi. Ωστόσο, αυτές οι τεχνικές μπορούν να εκτελεστούν μόνο αν ο διακομιστής είναι ικανός να δημιουργήσει DNS ή HTTP επερωτήσεις δεδομένων, έτσι ώστε να μεταφέρει δεδομένα στον επιτιθέμενο. Επομένως, η εν λόγω τεχνική χρησιμοποιείται κυρίως ως εναλλακτική λύση των δύο προαναφερθέντων τεχνικών, δηλαδή της In-band SQLi και της Inferential SQLi (Learning Center, 2023a).

2.6.3 Cross Site Scripting (XSS)

Οι επιθέσεις γνωστές ως Cross-site scripting (XSS) περιλαμβάνουν την έγχυση κακόβουλου κώδικα σε ιστότοπους, ο οποίος στη συνέχεια γίνεται μέρος του κώδικα που μεταδίδεται και εκτελείται από τον υπολογιστή του χρήστη. Το πρόγραμμα περιήγησης δεν έχει κανέναν τρόπο να γνωρίζει ότι τα κακόβουλα σενάρια είναι πράγματι κακόβουλα και ως εκ τούτου τα εκτελεί. Ως αποτέλεσμα, κακόβουλα σενάρια μπορούν να αποκτήσουν πρόσβαση σε διακριτικά περιόδου λειτουργίας ή άλλες ευαίσθητες πληροφορίες που διατηρούνται από το πρόγραμμα περιήγησης και χρησιμοποιούνται στον ιστότοπο. Επιπλέον, οι επιθέσεις XSS μπορούν να χρησιμοποιηθούν για τη διάδοση κακόβουλου λογισμικού, την τροποποίηση του κώδικα ιστότοπων, την πρόκληση προβλημάτων στα κοινωνικά δίκτυα ή ακόμη και την πραγματοποίηση επιθέσεων phishing.

Μια θεμελιώδης διαφορά σε σύγκριση με άλλους τύπους επιθέσεων είναι ότι ο στόχος της επίθεσης δεν είναι ο ιστότοπος ή ο διακομιστής στον οποίο φιλοξενείται, αλλά οι χρήστες του ιστότοπου. Στη δέσμη ενεργειών μεταξύ τοποθεσιών, ο εισβολέας εκμεταλλεύεται τα τρωτά σημεία σε έναν ιστότοπο, κάνοντάς τον να παραδίδει κακόβουλο κώδικα στους χρήστες. Αυτό συχνά περιλαμβάνει JavaScript ή οποιαδήποτε άλλη γλώσσα πελάτη. Οι κυβερνοεγκληματίες στοχεύουν ιστότοπους με ευάλωτες λειτουργίες που δέχονται δεδομένα εισόδου από τον χρήστη, όπως γραμμές αναζήτησης, πλαίσια σχολίων και φόρμες σύνδεσης.

Ανάλογα με τον τρόπο εισαγωγής του κώδικα και το κακόβουλο περιεχόμενο, μπορεί να μην βρίσκεται στον ίδιο τον ιστότοπο αλλά ως προσωρινό στοιχείο που φαίνεται να αποτελεί μέρος του ιστότοπου. Αυτά τα προσωρινά, μεταβατικά στοιχεία χρησιμοποιούνται συνήθως για την εμφάνιση πληροφοριών σε συγκεκριμένα άτομα ή για προσωρινή αποθήκευση δεδομένων.

Υπάρχουν διάφοροι τρόποι για να ενεργοποιήσετε μια επίθεση δέσμης ενεργειών μεταξύ τοποθεσιών. Για παράδειγμα, η εκτέλεση μπορεί να πραγματοποιηθεί αυτόματα κατά τη φόρτωση της σελίδας ή όταν ο χρήστης τοποθετεί το δείκτη του ποντικιού πάνω από ένα συγκεκριμένο στοιχείο, όπως μια υπερσύνδεση. Σε ορισμένες περιπτώσεις, μια επίθεση δέσμης ενεργειών μεταξύ τοποθεσιών μπορεί να εκτελεστεί με πιο άμεσο τρόπο, όπως μέσω email. Ορισμένες επιθέσεις XSS δεν έχουν συγκεκριμένο στόχο, αλλά μάλλον ο εισβολέας

εκμεταλλεύεται έναν ευάλωτο ιστότοπο για να «πιάσει» όσο το δυνατόν περισσότερα θύματα (Kaspersky, 2023b).

Οι τύποι επιθέσεων XSS είναι οι εξής:

- ***Stored cross-site scripting (Persistent XSS):*** Το αποθηκευμένο XSS, γνωστό και ως Persistent XSS, θεωρείται ο πιο καταστροφικός τύπος επίθεσης XSS. Μια επίθεση Αποθηκευμένου XSS συμβαίνει όταν τα δεδομένα χρήστη αποθηκεύονται και υποβάλλονται σε επεξεργασία σε έναν ιστότοπο. Τα τυπικά σημεία εισόδου για τέτοιες επιθέσεις περιλαμβάνουν φόρουμ μηνυμάτων, σχόλια ιστολογίου, προφίλ χρηστών και ονόματα χρηστών. Ο εισβολέας εκμεταλλεύεται αυτήν την ευπάθεια εισάγοντας ωφέλιμα φορτία XSS σε δημοφιλείς υποσελίδες ιστότοπου ή εξαπατώντας το θύμα να επισκεφτεί μια υποσελίδα που περιέχει τα αποθηκευμένα φορτία XSS, μεταδίδοντας και εκτελώντας έτσι τον κακόβουλο κώδικα στον υπολογιστή του χρήστη (Kaspersky, 2023b).
- ***Reflected Cross-Site Scripting (Non-persistent XSS):*** Το Reflected XSS είναι ο πιο κοινός τύπος επίθεσης XSS. Σε αυτήν την περίπτωση, ο κακόβουλος κώδικας του εισβολέα πρέπει να αποτελεί μέρος του ερωτήματος που αποστέλλεται στον διακομιστή ιστού. Αυτό αντικατοπτρίζεται έτσι ώστε η απόκριση HTTP να περιλαμβάνει τον κακόβουλο κώδικα του ερωτήματος HTTP. Ο εισβολέας χρησιμοποιεί κακόβουλους συνδέσμους, μηνύματα ηλεκτρονικού ψαρέματος και άλλες τεχνικές κοινωνικής μηχανικής για να ξεγελάσει το θύμα και να στείλει ένα αίτημα στον διακομιστή. Το ανακλώμενο ωφέλιμο φορτίο XSS εκτελείται στο πρόγραμμα περιήγησης του θύματος. Οι επιθέσεις XSS που αντανακλώνται απαιτούν ένα ευρύ φάσμα στόχων για να είναι αποτελεσματικές, επομένως ο εισβολέας πρέπει να παραδώσει τον κακόβουλο κώδικα σε κάθε θύμα ξεχωριστά. Αυτές οι επιθέσεις συχνά πραγματοποιούνται μέσω κοινωνικών δικτύων (Kaspersky, 2023b).
- ***DOM-based cross-site scripting***: Μια επίθεση DOM XSS συμβαίνει όταν μια εφαρμογή Ιστού εγγράφει δεδομένα στο μοντέλο αντικειμένου εγγράφου (DOM) χωρίς να τα ελέγχει. Το DOM είναι ένα αρχείο που χρησιμοποιείται για την ομαλή λειτουργία διαδικτυακών εφαρμογών. Μια διαδικτυακή εφαρμογή αποτελείται από τρία αρχεία: HTML, το οποίο αντιπροσωπεύει τη δομή της ιστοσελίδας, CSS, το οποίο

είναι υπεύθυνο για την οπτική αναπαράσταση της σελίδας και JavaScript, η οποία χειρίζεται τα δεδομένα της εφαρμογής. Για την αποτελεσματική επεξεργασία των δεδομένων, δημιουργείται το αρχείο DOM, το οποίο αντιπροσωπεύει τη σελίδα ως ένα σύνολο δομών δεδομένων. Επιτρέπει την τροποποίηση της σελίδας χωρίς να χρειάζεται να κάνετε αλλαγές στο HTML. Σε μια επίθεση DOM, τα κακόβουλα δεδομένα εκτελούνται μέσω του προγράμματος περιήγησης, συνήθως με τη μορφή ενός σεναρίου. Ένα κοινό σημείο επίθεσης είναι η διεύθυνση URL. Η εκτέλεση ενός κακόβουλου σεναρίου αναγκάζει το πρόγραμμα περιήγησης να εκτελεί κώδικα χωρίς την άδεια του χρήστη. Προκαλεί την εκτέλεση του κώδικα του ιστότοπου με τρόπο διαφορετικό από τον αναμενόμενο χωρίς να αλλάζει η εμφάνιση του ιστότοπου και να προκαλεί υποψίες στον χρήστη. Σε αντίθεση με τις επιθέσεις Αποθηκευμένες και Ανακλασμένες που απαιτούν την εκτέλεση ενός διακομιστή, μια επίθεση DOM πραγματοποιείται τοπικά μέσω του προγράμματος περιήγησης (PortSwigger, 2023; Kaspersky, 2023b).

- ***Blind Cross-Site Scripting***: Το Blind XSS scripting είναι μια μορφή αυτόματης επαναλαμβανόμενης επίθεσης XSS. Συνήθως συμβαίνει όταν το ωφέλιμο φορτίο του εισβολέα αποθηκεύεται στον διακομιστή και αποστέλλεται στο θύμα μέσω του backend του ιστότοπου. Για παράδειγμα, στις φόρμες σχολίων, οι εισβολείς μπορούν να περιλαμβάνουν κακόβουλα ωφέλιμα φορτία χρησιμοποιώντας τη φόρμα. Όταν ο χρήστης/διαχειριστής ανοίγει την υποβληθείσα φόρμα, εκτελείται το ωφέλιμο φορτίο του εισβολέα (Kirsten, 2023).

Μια επιτυχημένη επίθεση XSS μπορεί να έχει καταστροφικές συνέπειες στη φήμη μιας διαδικτυακής επιχείρησης και στη σχέση της με τους πελάτες της. Δυστυχώς, τα τρωτά σημεία που επιτρέπουν επιθέσεις XSS είναι ευρέως διαδεδομένα. Με την εκμετάλλευση αυτών των τρωτών σημείων, οι εισβολείς μπορούν να εκτελέσουν μια σειρά από κακόβουλες ενέργειες, όπως (Kaspersky, 2023b):

- Ανακατεύθυνση χρηστών σε κακόβουλες ιστοσελίδες.
- Καταγραφή οτιδήποτε πληκτρολογεί ο χρήστης.
- Πρόσβαση στο ιστορικό browser και στα περιεχόμενα του clipboard.
- Τρέξιμο web browser-based exploits.

- Απόκτηση πληροφοριών από τα cookies του χρήστη που είναι συνδεδεμένος σε μία ιστοσελίδα.
- Κλοπή login session token, επιτρέποντας στο θύμα να χρησιμοποιήσει την εφαρμογή χωρίς όμως το θύμα να ξέρει τους κωδικούς.
- Να αναγκάσει τον υπολογιστή του χρήστη να αποστείλει επερωτήσεις στο server υπό τον έλεγχο του επιτιθέμενου.
- Να αλλάξει τα περιεχόμενα μια σελίδας.
- Να κοροϊδέψει τα θύματα στο να δώσουν τον κωδικό ασφαλείας τους για την ιστοσελίδα σε άλλη ιστοσελίδα.
- Να μολύνουν το χρήστη με malware χρησιμοποιώντας αδυναμίες στο browser.

2.7 Disinformation - Misinformation

Η παραπληροφόρηση/ψευδή πληροφόρηση, είναι μια νέα μορφή επίθεσης που περιλαμβάνει τη διάδοση αλλοιωμένων πληροφοριών. Η δημοτικότητά της έχει αυξηθεί λόγω της αυξημένης χρήσης των πλατφορμών κοινωνικής δικτύωσης, ειδικά κατά τη διάρκεια της πανδημίας COVID-19. Αυτές οι επιθέσεις στοχεύουν στη μείωση της εμπιστοσύνης σε έναν οργανισμό, καθιστώντας τους απειλή υψηλού κινδύνου για την ασφάλεια στον κυβερνοχώρο.

Η ψευδή πληροφόρηση είναι μια σκόπιμη επίθεση που συνίσταται στην κατασκευή και διανομή ψευδών πληροφοριών. Τέτοιες επιθέσεις έχουν αυξηθεί σημαντικά κατά τη διάρκεια της πανδημίας, όπως αυτές που στοχεύουν στην εμπιστοσύνη των εμβολίων. Η παραπληροφόρηση, από την άλλη πλευρά, είναι μια ακούσια επίθεση όπου η διάδοση εσφαλμένων πληροφοριών συμβαίνει κατά λάθος. Η ανακρίβεια των δεδομένων είναι ακούσια και μπορεί να προκύψει για διάφορους λόγους.

Η συσχέτιση αυτών των απειλών με την κυβερνοασφάλεια δεν είναι άμεση. Ωστόσο, είναι σημαντικό να σημειωθεί ότι η παραπληροφόρηση και η ψευδή πληροφόρηση χρησιμοποιούνται συνήθως ως βάσεις για άλλες επιθέσεις, όπως phishing, κακόβουλο λογισμικό κ.λπ. Επιπλέον, τέτοιες απειλές μπορούν να χρησιμοποιηθούν ταυτόχρονα με άλλες επιθέσεις στον κυβερνοχώρο, δημιουργώντας υβριδικές απειλές. Ο πρωταρχικός σκοπός τους είναι να υπονομεύσουν την εμπιστοσύνη, τον θεμελιώδη ακρογωνιαίο λίθο της κυβερνοασφάλειας.

Η υψηλή ταχύτητα με την οποία διαδίδονται πληροφορίες μέσω του διαδικτύου, κυρίως αλλά όχι αποκλειστικά μέσω των μέσων κοινωνικής δικτύωσης, παρέχει πρόσφορο έδαφος για επιθέσεις παραπληροφόρησης/ψευδή πληροφόρησης. Η διάδοση και η επιτυχία αυτών των επιθέσεων είναι συνάρτηση πολλών παραγόντων. Κατανοώντας την ευκολία που προσφέρει η σύγχρονη ψηφιακή επικοινωνία σχετικά με την ταχύτητα και την εμβέλεια της διάδοσης πληροφοριών, κατανοούμε και το μέγεθος της πιθανής βλάβης. Σημαντική είναι και η τεχνολογική διάσταση που γίνεται σε θέματα που οδηγούν σε περιφρόνηση. Πολύ συχνά, ασήμαντα προβλήματα μεγεθύνονται στις πλατφόρμες των μέσων κοινωνικής δικτύωσης και μερικές φορές διαδίδονται αμφίβολες ειδήσεις υπό το πέπλο της ανωνυμίας.

Επιπλέον, δεν είναι ασυνήθιστο για τις τεχνικές λειτουργίες ενός συστήματος να δημιουργούν λίστες με θεματικά θέματα, κάτι που οδηγεί σε περαιτέρω διασπορά. Κατά συνέπεια, οι άνθρωποι εκτίθενται σε ομάδες που μοιράζονται τις ίδιες πεποιθήσεις και αντιμετωπίζουν καταστάσεις ή προβλήματα με την ίδια ή παρόμοια αντίληψη όταν επικοινωνούν, ενισχύοντας το περιεχόμενο της παραπληροφόρησης μέσω της συνεχούς αναπαραγωγής εμπρός-πίσω, δημιουργώντας έτσι το φαινόμενο του «Echo Chamber».

Πολλοί ιστότοποι καταφεύγουν σε τεχνικές clickbait για να δημιουργήσουν περισσότερα κέρδη, δημιουργώντας άρθρα με διογκωμένους ή ακόμα και κατασκευασμένους τίτλους για να προσελκύσουν πιθανούς αναγνώστες και να τους ενθαρρύνουν να κάνουν κλικ στο χαρτί. Ωστόσο, καθώς πολλοί άνθρωποι τείνουν να διαβάζουν μόνο τον τίτλο του άρθρου, αυτό οδηγεί συχνά σε παρανοήσεις και παραπληροφόρηση. Η πολυπλοκότητα αυτών των απειλών είναι σημαντική, καθώς είναι δύσκολο να διακρίνει κανείς τον πραγματικό σκοπό των πληροφοριών ή την πηγή. Αυτό γίνεται ακόμη πιο δύσκολο όταν εκστρατείες ψευδής πληροφόρησης σχεδιάζονται σχολαστικά και η ύπαρξη διαφορετικών παράλληλων εκστρατειών ψευδής πληροφόρησης περιπλέκει περαιτέρω το θέμα, καθιστώντας δύσκολη τη χάραξη ορίων μεταξύ τους. Για παράδειγμα, οι διαφορές μεταξύ διαφήμισης, δημοσίων σχέσεων και προπαγάνδας δεν είναι πάντα εμφανείς, καθώς όλες οι καμπάνιες εξαρτώνται από την ατομική ερμηνεία.

Ο κύριος στόχος αυτών των απειλών είναι να πλημμυρίσουν το κοινό με ψευδείς ειδήσεις για να προκαλέσουν αβεβαιότητα και αδιαφορία για την αλήθεια. Δημιουργούν τόσο περίπλοκες καταστάσεις που η αναζήτηση της αλήθειας γίνεται τρομακτική. Χρησιμοποιούνται επίσης για να προκαλέσουν φόβο και κοινωνική ένταση που μπορεί να οδηγήσει στον κατακερματισμό των κοινωνικών ομάδων. Για το λόγο αυτό, νομοθέτες σε πολλές χώρες έχουν θέσει την παραπληροφόρηση/ψευδή πληροφόρηση στο επίκεντρο της ατζέντας τους και έχουν αρχίσει να λαμβάνουν μέτρα για τον περιορισμό των ψευδών ειδήσεων, μερικές φορές μάλιστα καταφεύγοντας στο φιλτράρισμά τους.

Οι κακόβουλες ομάδες είναι συνήθως υπεύθυνες για τη διάδοση παραπληροφόρησης και ψευδών πληροφοριών. Από τη μία πλευρά, υπάρχουν ομάδες που υποστηρίζονται από τις κυβερνήσεις. Από την άλλη πλευρά, οι εγκληματίες του κυβερνοχώρου μπορεί να είναι ιδιωτικοί οργανισμοί. Για παράδειγμα, οι θεωρίες συνωμοσίας μοιράζονται τρομοκράτες,

εξτρεμιστές και οργανωμένους εγκληματίες για να χειραγωγήσουν ανθρώπους. Γενικά, μεγάλο μέρος αυτών των επιθέσεων πραγματοποιείται από μη κρατικές εσωτερικές οντότητες. Και οι δύο οντότητες στοχεύουν τον ιδιωτικό τομέα με αυξανόμενο ρυθμό για τη διάδοση παραπληροφόρησης για τη χειραγώγηση των αγορών ή την επίθεση στη φήμη των ανταγωνιστών. Η παραπληροφόρηση και οι ψευδείς πληροφορίες μοιράζονται με αυξανόμενο ρυθμό μέσω αλυσίδων μηνυμάτων, περιεχομένου μέσων κοινωνικής δικτύωσης και phishing μέσω φωνής, κειμένου και ηλεκτρονικού ταχυδρομείου (ENISA, 2021).

Επιπλέον, υπάρχουν οργανωμένες ομάδες που προσφέρουν παραπληροφόρηση και ψευδείς ειδήσεις ως υπηρεσία, γνωστές ως Παραπληροφόρηση ως Υπηρεσία. Η ταχεία εξέλιξη της τεχνητής νοημοσύνης (AI) είναι ένας άλλος παράγοντας. Η τεχνητή νοημοσύνη χρησιμοποιείται για τη δημιουργία ρεαλιστικών προφίλ και εικόνων και για την τροποποίηση περιεχομένου και εικόνων σε αναρτήσεις χωρίς να εντοπίζονται. Αυτός ο τύπος περιεχομένου ονομάζεται "Συνθετικά Μέσα". Επιπλέον, πολλοί από τους αλγόριθμους που χρησιμοποιούνται σήμερα σε ιστότοπους για τον προσδιορισμό του περιεχομένου που βλέπει κάθε χρήστης βασίζονται σε μορφές τεχνητής νοημοσύνης.

Μία από τις πιο εντυπωσιακές εφαρμογές της τεχνητής νοημοσύνης είναι η δημιουργία των λεγόμενων Deepfakes, τα οποία είναι ψηφιακά πρόσωπα που μοιάζουν πανομοιότυπα με αυτά των πραγματικών ανθρώπων, που δημιουργούνται μέσω αλγορίθμων AI. Είναι επίσης δυνατό να δημιουργήσετε ψεύτικα ηχητικά μηνύματα ή ακόμα και εικόνες με αληθινά άτομα που δεν συμμετείχαν ποτέ σε αυτά τα μηνύματα. Ως αποτέλεσμα, οι εκστρατείες παραπληροφόρησης και ψευδούς πληροφόρησης γίνονται όλο και πιο αποτελεσματικές λόγω των deepfakes, που είναι δύσκολο να καταπολεμηθούν. Ένα παράδειγμα χρήσης του Deepfake είναι η προσπάθεια των ρωσικών στρατευμάτων να προκαλέσουν την παράδοση των ουκρανικών στρατευμάτων χρησιμοποιώντας ένα ψεύτικο μήνυμα, Deepfake, από τον Πρωθυπουργό της Ουκρανίας (Holroyd, 2022).

Υπάρχουν διάφορες τεχνικές για τη δημιουργία deepfakes. Το πρώτο και παλαιότερο είναι το face swapping, το οποίο χρησιμοποιήθηκε πριν από την εμφάνιση των τεχνολογιών μηχανικής εκμάθησης και χρησιμοποιούσε προγράμματα επεξεργασίας εικόνας όπως το Gimp και το Photoshop. Μέσω αυτών των προγραμμάτων, ο καθένας μπορούσε να μεταφέρει το πρόσωπο ενός ατόμου στο σώμα κάποιου άλλου.

Οι πιο σύγχρονες τεχνικές χρησιμοποιούν προγράμματα μηχανικής εκμάθησης για να δημιουργήσουν ακόμα πιο πειστικά deepfakes. Χρησιμοποιούν είτε κωδικοποιητές είτε Deep Neural Networks (DNN). Για να μάθετε την εναλλαγή προσώπων, χρησιμοποιείται ένας αυτόματος κωδικοποιητής. Τα προεπεξεργασμένα δείγματα από τις δύο όψεις χαρτογραφούνται χρησιμοποιώντας τις ίδιες παραμέτρους κωδικοποιητή. Αφού τα δίκτυα εκπαιδεύονται στην εναλλαγή μπροστινών, ένα βίντεο ή μια εικόνα της εμφάνισης που πρόκειται να μιμηθεί εισέρχεται σε έναν κωδικοποιητή. Στην περίπτωση βίντεο, η είσοδος γίνεται καρέ-καρέ. Στη συνέχεια, αποκωδικοποιείται και εφαρμόζεται στο βίντεο ή στην εικόνα που πρόκειται να χειριστείτε. Αρκετές εφαρμογές επιτρέπουν την εναλλαγή προσώπων, αλλά δεν χρησιμοποιούν όλες τους ίδιους αλγόριθμους.

Μια άλλη τεχνική είναι το Lip Syncing, το οποίο αντιστοιχίζει μια ηχογραφημένη φωνή σε ένα βίντεο, έτσι ώστε το εικονιζόμενο πρόσωπο «να φαίνεται» να λέει κάτι αληθινό. Επιτρέπει σε κάποιον να κάνει τον στόχο να πει αυτό που θέλει. Αυτή η τεχνική μπορεί να συνδυαστεί με αντικατάσταση προσώπου για να δημιουργήσετε μια εντελώς ψεύτικη εικόνα.

Μια τεχνική που χρησιμοποιείται στη βαθιά μάθηση είναι η τεχνική «μαριονέτας». Αυτή η τεχνική επιτρέπει στο χρήστη να κάνει το αντικείμενο-στόχο να κινείται με διαφορετικό τρόπο από την αρχική του κίνηση. Αυτό μπορεί να περιλαμβάνει κινήσεις του προσώπου ή ακόμα και κινήσεις ολόκληρου του σώματος. Η τεχνική μαριονέτας χρησιμοποιεί κυρίως την τεχνολογία Generative Adversarial Network (GAN). Η τεχνική βασίζεται στη χρήση δύο ξεχωριστών δικτύων μηχανικής μάθησης που έχουν ανταγωνιστική σχέση. Το πρώτο δίκτυο λειτουργεί ως «γεννήτρια». Τα δεδομένα που αντιπροσωπεύουν το αντικείμενο που πρόκειται να αναπαραχθεί εισάγονται στο πρώτο δίκτυο έτσι ώστε να μπορεί να μάθει τα χαρακτηριστικά του. Μετά τη λήψη αυτών των δεδομένων, το δίκτυο παράγει διάφορα παραδείγματα και απομιμήσεις, τα οποία έχουν τα ίδια χαρακτηριστικά με την πηγή. Στη συνέχεια, αυτά τα δεδομένα εισάγονται στο δεύτερο δίκτυο, το οποίο είναι εκπαιδευμένο να αναγνωρίζει αυτά τα χαρακτηριστικά. Το δεύτερο δίκτυο ονομάζεται “διάκριση” και είναι υπεύθυνο για την εξέταση όλων των παραδειγμάτων που δημιουργούνται από το πρώτο δίκτυο για να εντοπίσει τυχόν ατέλειες που θα μπορούσαν να κάνουν τους ανθρώπους να συνειδητοποιήσουν ότι πρόκειται για μίμηση. Οποιαδήποτε παραδείγματα διαπιστωθεί ότι

έχουν ελαττώματα αποστέλλονται πίσω στο πρώτο δίκτυο για να βελτιωθούν. Αυτή η επαναληπτική διαδικασία συνεχίζεται μέχρι να δημιουργηθεί το βέλτιστο δυνατό δείγμα.

Μια αρκετά σημαντική συνέπεια των τεχνικών πρόσωπο με πρόσωπο είναι η μίμηση πολιτικών προσώπων για τη διάδοση ψευδών πληροφοριών. Ανάλογα με την περίπτωση, αυτό μπορεί να έχει σοβαρές συνέπειες. Μια άλλη επιβλαβής χρήση είναι στην πορνογραφία, όπου χρησιμοποιούνται τεχνολογίες αλλαγής προσώπου για την κατασκευή του προσώπου δημοφιλών γυναικών. Αυτές οι γυναίκες δεν έχουν τρόπο να αποτρέψουν τη δημιουργία αυτού του πορνογραφικού υλικού (DHS GOV, 2018).

2.8 Non-Malicious Threats

Σε αυτή την κατηγορία περιλαμβάνονται απειλές που δεν προέρχονται από ενέργειες κακόβουλου παράγοντα. Τα ανθρώπινα λάθη και η κακή διαχείριση ενός συστήματος τα προκαλούν. Στον τομέα της κυβερνοασφάλειας, λέγεται συχνά ότι οι άνθρωποι είναι ο πιο αδύναμος κρίκος ενός συστήματος. Οι κύριοι λόγοι για αυτό είναι η έλλειψη εκπαίδευσης και ευαισθητοποίησης μεταξύ των χρηστών, των προγραμματιστών και των διαχειριστών. Η έλλειψη τυποποιημένων διαδικασιών, καθώς και η αυξανόμενη πολυπλοκότητα των σύγχρονων συστημάτων, αυξάνει την πιθανότητα σφαλμάτων. Περιλαμβάνονται επίσης οι φυσικές καταστροφές που ενδέχεται να επηρεάσουν τα πληροφοριακά συστήματα. Λόγω της φύσης τους, αυτές οι απειλές έχουν μόνιμη ύπαρξη και είναι εξαιρετικά σημαντικές. Μπορούν να χωριστούν σε δύο κατηγορίες (ENISA, 2021):

1. Απροσεξίες και σφάλματα: Προκαλούνται από αφέλεια, έλλειψη επίγνωσης ή είναι απλά ανθρώπινα λάθη. Περιλαμβάνουν:
    a. Λάθη στην διαχείριση ενός πληροφοριακού συστήματος, όπως:
        i. Άστοχες ρυθμίσεις όταν εφαρμογές και συστήματα επαναρυθμίζονται ή ανανεώνονται. Πολλές φόρες μια ανανέωση ή επαναρύθμιση μπορεί να αλλάξει μια ρύθμιση ασφαλείας, κάτι που μπορεί να δημιουργήσει μια αδυναμία στο σύστημα.
        ii. Κακοδιαχείριση του συστήματος συμπεριλαμβανομένων λαθών σε patching και ανανεώσεις συστήματος. Μη ενημερωμένα συστήματα πολλές φορές είναι ευάλωτα σε καινούργιες παραλλαγές επιθέσεων.
        iii. Κακοδιαχείριση σε επίπεδο Διαχειριστή, για παράδειγμα διαμοίραση προνομίων σε χρήστες που δεν θα έπρεπε να τα έχουν. Έτσι δίνεται πρόσβαση σε διαβαθμισμένα αρχεία σε άτομα που δεν θα έπρεπε να έχουν κάτι που μπορεί να οδήγηση σε διαρροή δεδομένων.
        iv. Προβλήματα στη διαχείριση παραδοσιακών συστημάτων όπως διαχείριση δικτύων, ελέγχου πρόσβασης και διαχείρισης ταυτοτήτων. Μπορούν να αποτελέσουν σημείο εισαγωγής για ένα επιτιθέμενο για διάφορες επιθέσεις.
2. Λάθη από προγραμματιστές (ENISA, 2021):

a. Προβλήματα με dependencies, για παράδειγμα απομείναντες βιβλιοθήκες που δεν χρησιμοποιούνται χωρίς να το καταλάβουν οι προγραμματιστές. Μπορούν αξιοποιηθούν από έναν επιτιθέμενο με κακόβουλο τρόπο.
b. Αβλεψίες όπως η αποθήκευση διαπιστευτηρίων για την ασφαλή πρόσβαση σε εφαρμογές σε δημόσια repositories και άλλα. Αυτό μπορεί να δώσει σε μία κακόβουλη οντότητα πρόσβαση σε πολύ σημαντικά πράγματα όπως πιστοποιητικά SSL κάτι που τους ανοίγει το δρόμο για αριθμό επιθέσεων.

- Λάθη σε επίπεδο εφαρμογής (ENISA, 2021):
    - Κακοδιαχείριση cloud εφαρμογών. Κακοδιαχείριση μπορεί να σημαίνει μη επίβλεψη πρόσβασης χρηστών , ροών δεδομένων , προστασία βάσεων δεδομένων κλπ. Αυτό μπορεί να οδήγηση στην παράβλεψη μη εγκεκριμένης πρόσβασης στο σύστημα , παράβλεψη σημαδιών επίθεσης DOS κλπ.
    - Φτωχή πολιτική διαχείρισης κωδικών και κλειδιών. Μοιρασμός κωδικών ασφαλείας και ειδικά διαβαθμισμένων κωδικών μπορεί να οδηγήσει σε αυθαίρετη πρόσβαση. Επίσης η επαναχρησιμοποίησή κωδικών, κυρίως μεταξύ δουλείας και προσωπικής ζωής καθώς και η μη αλλαγή κωδικών μπορεί να προκαλέσει πρόβλημα ειδικά αν ο κωδικός έχει διαρρεύσει.
    - Μικρά λάθη όπως η αποστολή email σε λάθος παραλήπτη. Η αποστολή διαβαθμισμένων πληροφορίων σε λάθος παραλήπτη μπορεί εύκολα οδηγήσει σε διαρροή.
- Λάθη σε φυσικό επίπεδο (ENISA, 2021):
    - Συσκευές που είναι ευάλωτες σε κλοπή πληροφοριών, όπως π.χ. USB sticks, εξωτερικοί σκληροί δίσκοι. Αυτές η συσκευές είναι πολύ εύκολο να κλαπούν εάν δεν φυλάσσονται κατάλληλα.
    - Εξαιρέσεις στη πρόσβαση σε φυσικούς χώρους. Η διαβαθμιζομένη πρόσβαση υπάρχει για να περιορίσει την πρόσβαση μόνο σε όσους χρειάζεται να βρίσκονται σε ένα χώρο για λόγους εργασίας, διασφαλίζοντας έτσι την προστασία των πληροφορίων σε ένα σημαντικό βαθμό. Κατ' εξαίρεση πρόσβαση μπορεί πολύ εύκολα να οδηγήσει σε πρόβλημα ασφαλείας μόνο και μόνο από μια μικρή απροσεξία.

- Φυσικές καταστροφές (ENISA, 2021):
    - Ζημίες στη φυσική υποδομή, όπως αναπόφευκτη χρονική φθορά στα καλώδια οπτικών ινών, απώλεια διαδικτυακής σύνδεσης, φωτιά, ασταθής πηγή ενέργειας.
    - Φυσικές καταστροφές, όπως πλημμύρες και σεισμοί.

Σε αυτού του είδους τις απειλές διακρίνονται τέσσερις διαφορετικές κατηγορίες οντοτήτων οι οποίες μπορεί να επηρεάσουν ένα σύστημα και να οδηγήσουν σε διαρροή δεδομένων και άλλες απειλές. Αυτές είναι οι εξής (ENISA, 2021):

1. Απλοί χρήστες που χρησιμοποιούν το σύστημα με όσα προνομία χρειάζονται για να εκτελέσουν μια συγκεκριμένη δουλειά σε αυτό.
2. Χρήστες με προνόμια (Διαχειριστές) οι οποίοι είναι υπεύθυνοι για τη ρύθμιση και διαχείριση του συστήματος. Λάθη από αυτές τις οντότητες προκαλούν και την μεγαλύτερη ζημιά.
3. Προγραμματιστές και μηχανικοί λογισμικού που σχεδιάζουν, υλοποιούν και προγραμματίζουν ένα σύστημα.
4. Service/Cloud providers προμηθεύουν μια cloud υπηρεσία ή λειτουργία η οποία ενσωματώνεται στο σύστημα.

Οι μη κακόβουλες απειλές αποτελούν το υπόστρωμα πάνω στο οποίο μπορούν να αναπτυχθούν οι κακόβουλες απειλές που αναφέρθηκαν στο προηγούμενα κεφάλαια. Για παράδειγμα, αδυναμίες ασφαλείας, άστοχες ρυθμίσεις, ανεπαρκής διαχείριση αδυναμιών και patching μπορούν να ανοίξουν την πόρτα σε DDoS επιθέσεις, malware, ransomware. Την ίδια στιγμή ανθρώπινα λάθη και απροσεξίες αποτελούν τη βάση για επιθέσεις phishing

2.9 Advanced Persistent Threats

Σε αυτή την κατηγορία περιλαμβάνονται τεχνικές συνεχούς, κρυφής και εξαιρετικά πολύπλοκης επίθεσης, οι οποίες στοχεύουν στην απόκτηση πρόσβασης στο σύστημα, καθώς και στη διατήρηση αυτής της πρόσβασης για μεγάλο χρονικό διάστημα, κάτι που μπορεί να έχει καταστροφικές συνέπειες.

1. ***Απόκτηση Πρόσβασης***

Χρησιμοποιώντας μη ασφαλή δίκτυα, μολυσμένα αρχεία, κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου ή ευπάθειες ασφαλείας εφαρμογών, οι εισβολείς εισάγουν κακόβουλο λογισμικό σε ένα σημείο του δικτύου στο οποίο θέλουν να αποκτήσουν πρόσβαση. Μπορούν επίσης να χρησιμοποιήσουν τακτικές εκτροπής, όπως μια επίθεση DDoS για να αποσπάσουν την προσοχή του προσωπικού ασφαλείας και να κάνουν τη διαδικασία απόκτησης πρόσβασης πιο εύκολη γι’ αυτούς (Kaspersky, 2023c· Learning Center, 2023b).

2. ***Δημιουργία Απρόσκοπτης Πρόσβασης***

Μετά την ενσωμάτωση κακόβουλου λογισμικού, οι εισβολείς δημιουργούν κερκόπορτες και σήραγγες που τους επιτρέπουν να κινούνται μέσα στο σύστημα χωρίς να εντοπιστούν. Αυτοί οι τύποι κακόβουλου λογισμικού χρησιμοποιούν τεχνικές όπως η επανεγγραφή κώδικα για να καλύψουν τα ίχνη των εισβολέων. Το κακόβουλο λογισμικό που δημιουργεί αυτές τις κερκόπορτες μπορεί να εγκατασταθεί με διάφορους τρόπους, όπως μέσω Trojan malware που μεταμφιέζεται ως νόμιμο λογισμικό ή μέσω ενημερώσεων σε υπάρχον λογισμικό (επίθεση στην αλυσίδα εφοδιασμού λογισμικού) (Kaspersky, 2023c·Learning Center, 2023b).

3. ***Επέκταση στο Σύστημα***

Όταν οι εισβολείς αποκτούν είσοδο σε ένα σύστημα, χρησιμοποιούν τεχνικές όπως το σπάσιμο κωδικού πρόσβασης για να αποκτήσουν δικαιώματα διαχειριστή για να έχουν περισσότερο έλεγχο και πρόσβαση σε όλες τις λειτουργίες του συστήματος. Αυτό περιλαμβάνει την απόκτηση πρόσβασης σε προσωπικούς λογαριασμούς που έχουν πρόσβαση σε ευαίσθητα και κρίσιμα δεδομένα, όπως πληροφορίες προϊόντων, δεδομένα εργαζομένων και οικονομικές πληροφορίες.

Ανάλογα με τον τελικό στόχο της επίθεσης, τα δεδομένα που συλλέγονται μπορεί να πωληθούν σε ανταγωνιστές, να ανταλλάσσονται για να υπονομεύσουν ένα προϊόν ή να χρησιμοποιηθούν για την καταστροφή του οργανισμού (π.χ. αναφορά παράνομων δραστηριοτήτων στις αρχές). Σε περίπτωση δολιοφθοράς, οι επιτιθέμενοι προσπαθούν να αποκτήσουν τον έλεγχο πολλών κρίσιμων συστημάτων για να προκαλέσουν όσο το δυνατόν μεγαλύτερη ζημιά. Για παράδειγμα, οι εισβολείς μπορούν να διαγράψουν ολόκληρες βάσεις δεδομένων προκαλώντας άλλους τύπους ζημιών στο δίκτυο, παρατείνοντας έτσι τη διαδικασία επαναφοράς των συστημάτων.

Σε αυτό το στάδιο, οι εισβολείς θα προσπαθήσουν επίσης να δημιουργήσουν περισσότερα σημεία πρόσβασης στο σύστημα, ώστε να υπάρχουν εναλλακτικές λύσεις σε περίπτωση που εντοπιστεί και κλείσει ένα υπάρχον σημείο πρόσβασης (Kaspersky, 2023c· Learning Center, 2023b· Crowdstrike, 2023).

4. Εξαγωγή Πληροφορίων

Κατά τη διάρκεια μιας επίθεσης APT, τα δεδομένα που θέλουν να κλέψουν οι εισβολείς αποθηκεύονται σε ασφαλείς τοποθεσίες εντός του δικτύου. Μόλις ολοκληρωθεί η συλλογή δεδομένων, πρέπει να εξαχθούν χωρίς να εντοπιστούν. Ο πιο συνηθισμένος τρόπος είναι να δημιουργήσετε "λευκό θόρυβο", μια εκτροπή, όπως μια επίθεση DDoS (Learning Center, 2023b· Crowdstrike, 2023).

Λόγω της πολυπλοκότητάς τους, αυτοί οι τύποι επιθέσεων στοχεύουν έθνη ή μεγάλες εταιρείες με στόχο την κλοπή πληροφοριών για μεγάλο χρονικό διάστημα. Ωστόσο, αυτό δεν σημαίνει ότι οι μικρές επιχειρήσεις μπορούν να αγνοήσουν αυτού του είδους τις επιθέσεις. Οι μικρότερες εταιρείες που αποτελούν μέρος μιας μεγαλύτερης αλυσίδας εφοδιασμού μπορούν να γίνουν στόχοι με στόχο να αποκτήσουν πρόσβαση στη μεγαλύτερη εταιρεία, δημιουργώντας μια επίθεση στην αλυσίδα εφοδιασμού όπως περιγράφεται παραπάνω. Οι μικρότερες εταιρείες συνήθως δεν προστατεύονται καλά από κακόβουλες επιθέσεις και χρησιμοποιούνται ως μεσάζοντες (Kaspersky, 2023c).

2.10 Virtualization

Η εικονικοποίηση έχει αποκτήσει περισσότερες δυνατότητες τα τελευταία χρόνια λόγω της ικανότητάς της να παρέχει βελτιωμένη αποτελεσματικότητα και επεκτασιμότητα με ταυτόχρονη μείωση του λειτουργικού κόστους. Η εικονικοποίηση χρησιμοποιεί λογισμικό για τη δημιουργία ενός εικονικού περιβάλλοντος όπου μπορούν να σχεδιαστούν και να εκτελεστούν πολλαπλές εικονικές μηχανές (VM). Κάθε VM εκτελεί το λειτουργικό του σύστημα και συμπεριφέρεται σαν ανεξάρτητος υπολογιστής (Atumu, 2021· IBM, 2023).

Σήμερα, η συντριπτική πλειοψηφία των οργανισμών χρησιμοποιεί εικονικοποίηση διακομιστή και πολλοί εξερευνούν άλλους τύπους εικονικοποίησης, συμπεριλαμβανομένης της εικονικοποίησης επιτραπέζιων υπολογιστών, εφαρμογών και αποθήκευσης. Ωστόσο, όπως όλες οι τεχνολογίες, η υιοθέτηση της εικονικοποίησης εγκυμονεί κινδύνους ασφαλείας.

- ***VM Sprawl:*** Η απουσία αυστηρών πολιτικών διαχείρισης VM εντός ενός οργανισμού μπορεί να οδηγήσει στο πρόβλημα της εξάπλωσης εικονικών μηχανών, που είναι η ανεξέλεγκτη δημιουργία VM. Αυτό μπορεί να οδηγήσει στην εξάντληση των διαθέσιμων πόρων των υπολογιστικών συστημάτων και σε μια μεγαλύτερη επιφάνεια επίθεσης μέσω των πολλών και συνήθως ανεπαρκώς προστατευμένων VMs (Penetration Testing Lab, 2013, Atumu, 2021).
- ***Malware***: Οι εικονικές μηχανές (VM), όπως οι παραδοσιακοί υπολογιστές, είναι ευάλωτες σε κακόβουλο λογισμικό. Αυτές οι επιθέσεις μπορεί να προέρχονται από μολυσμένες εικόνες VM ή υπαλλήλους χωρίς την απαραίτητη εκπαίδευση ασφαλείας. Εάν ένα VM μολυνθεί, μπορεί να «μολύνει» ολόκληρη την ψηφιακή υποδομή ενός οργανισμού (Penetration Testing Lab, 2013, Atumu, 2021).
- ***Network configuration***: Η κακή διαμόρφωση, όπως η δυνατότητα μεταφοράς αρχείων μεταξύ εικονικών μηχανών ή ανοιχτών θυρών τείχους προστασίας, μπορεί να είναι αρκετή για να αποκτήσει πρόσβαση ένας εισβολέας σε μια ψηφιακή υποδομή. Αυτό περιλαμβάνει φυσικούς διακομιστές, οι οποίοι χωρίς τις απαραίτητες ενημερώσεις, μπορούν να δημιουργήσουν πρόβλημα ασφαλείας (Εργαστήριο δοκιμών διείσδυσης, 2013, Atumu, 2021).

- ***Access Control***: Ένας εισβολέας αποκτά πρόσβαση στην εικονική υποδομή αποκτώντας φυσική πρόσβαση στους διακομιστές ή μέσω ενός παραβιασμένου λογαριασμού στην πλατφόρμα διαχείρισης VM (Penetration Testing Lab, 2013, Atumu, 2021).
- ***Security of Offline Virtual Machines***: Η δημιουργία αντιγράφων ασφαλείας εκτός σύνδεσης ή εκτός τοποθεσίας είναι απαραίτητη για την πολιτική Αντιμετώπισης περιστατικών, ακριβώς για το στάδιο της αποκατάστασης. Ωστόσο, όταν δημιουργείται αντίγραφο ασφαλείας ενός VM, οι ρυθμίσεις ασφαλείας και οι ενημερώσεις είναι εκείνες που είχε όταν ήταν για τελευταία φορά ενεργό. Επομένως, εάν επανενεργοποιηθεί, οι ρυθμίσεις μπορεί να είναι ξεπερασμένες, γεγονός που μπορεί να θέσει σε κίνδυνο το υπόλοιπο ψηφιακό περιβάλλον (Penetration Testing Lab, 2013· Atumu, 2021).
- ***Workloads with Different Trust Levels***: Χωρίς κατάλληλους ελέγχους ασφαλείας, είναι δυνατή η δημιουργία δοκιμαστικού διακομιστή στο ίδιο περιβάλλον με έναν διακομιστή παραγωγής που περιέχει ευαίσθητες πληροφορίες. Οι δοκιμαστικοί διακομιστές συνήθως δεν απαιτούν υψηλά επίπεδα ασφάλειας, καθώς δημιουργούνται προσωρινά για δοκιμή. Επομένως, εάν βρίσκονται στο ίδιο περιβάλλον με άλλους διακομιστές παραγωγής, μπορεί να είναι ένα κενό ασφαλείας (Penetration Testing Lab, 2013; Atumu, 2021).
- ***Hypervisor Security Controls***: Ο hypervisor είναι η πλατφόρμα που επιτρέπει στα VM να λειτουργούν σε κοινόχρηστο υλικό. Επομένως, μπορεί να είναι ένα μόνο σημείο αποτυχίας για ολόκληρη την εικονική υποδομή. Αυτή η επίθεση είναι γνωστή ως Hyperjacking (Εργαστήριο δοκιμών διείσδυσης, 2013; Atumu, 2021).
- ***Cloud Service Provider APIs***: Για οργανισμούς που εκτελούν υβριδικά μοντέλα που περιλαμβάνουν δημόσιες και ιδιωτικές υποδομές, οι επιθέσεις μέσω του API του παρόχου υπηρεσιών cloud είναι επικίνδυνες. Αυτά τα API στοχεύουν στη διευκόλυνση της αποτελεσματικής επικοινωνίας μεταξύ των δύο περιβαλλόντων, επομένως υπάρχει κίνδυνος εάν δεν είναι επαρκώς ασφαλισμένα (Penetration Testing Lab, 2013· Atumu, 2021).
- ***VM Escape***: Ένα λειτουργικό σύστημα «ξεφεύγει» από τη φούσκα ασφαλείας στην οποία βρίσκεται ένα VM και επικοινωνεί απευθείας με τον hypervisor. Αυτό μπορεί

να δώσει στον εισβολέα τη δυνατότητα πρόσβασης σε όλα τα VM που εκτελούνται σε αυτόν τον διακομιστή και πρόσβαση στον ίδιο τον κεντρικό διακομιστή, εάν τα προνόμια είναι αρκετά υψηλά (Penetration Testing Lab, 2013; Atumu, 2021).

ΚΕΦΑΛΑΙΟ 3. Internet-of-Things (IoT)

Ο όρος “Internet of Things” (IoT) περιλαμβάνει όλες τις συσκευές που είναι συνδεδεμένες στο Διαδίκτυο που δεν είναι παραδοσιακοί υπολογιστές (δηλαδή επιτραπέζιοι και φορητοί υπολογιστές). Αυτό μπορεί να περιλαμβάνει οτιδήποτε, από ιχνηλάτες φυσικής κατάστασης και έξυπνα ρολόγια έως έξυπνα ψυγεία, κάμερες, πλυντήρια ρούχων, αυτοκίνητα, φανάρια και συστήματα οικιακής ασφάλειας. Καθώς το διαδίκτυο γίνεται πιο προσιτό και τα ολοκληρωμένα κυκλώματα γίνονται πιο προσιτά, δημιουργούνται περισσότερες διασυνδεδεμένες συσκευές και εμπίπτουν στην κατηγορία IoT. Ενώ αυτές οι συσκευές προσφέρουν πολλά οφέλη στους χρήστες όσον αφορά τη λειτουργικότητά τους, μπορούν επίσης να στοχοποιηθούν από εγκληματίες του κυβερνοχώρου, όπως τα παραδοσιακά συστήματα υπολογιστών. Επομένως, πρέπει να ληφθούν τα κατάλληλα μέτρα ασφαλείας. Οι απειλές για τα συστήματα IoT είναι σημαντικές λόγω των ειδικών χαρακτηριστικών αυτής της τεχνολογίας που επιτρέπουν στα περιβάλλοντα IoT να λειτουργούν αποτελεσματικά και αποδοτικά. Ωστόσο, αυτά τα χαρακτηριστικά τα καθιστούν ευάλωτα στην εκμετάλλευση από εγκληματίες του κυβερνοχώρου (Coudflare, 2023· TrendMicro, 2023). Αυτά είναι:

- ***Συλλογή Δεδομένων***

Οι IoT συσκευές και αισθητήρες συλλέγουν δεδομένα εκτενούς λεπτομέρειας από το περιβάλλον και τους χρήστες τους, τα οποία είναι απαραίτητα για τη λειτουργία των περιβαλλόντων IoT. Ωστόσο, εάν αυτά τα δεδομένα δεν προστατευθούν σωστά και κλαπούν, τότε θα υπάρχουν σημαντικές νομικές συνέπειες (TrendMicro, 2023).

- ***Σύνδεση φυσικού και ψηφιακού περιβάλλοντος***

Πολλές συσκευές IoT μπορούν να λειτουργήσουν μέσω δεδομένων που συλλέγονται από το περιβάλλον τους, μειώνοντας την απόσταση μεταξύ ψηφιακών και φυσικών συστημάτων. Ωστόσο, εάν αυτά τα δεδομένα δεν προστατεύονται επαρκώς και κλαπούν, μπορεί να υπάρξουν σημαντικές νομικές συνέπειες (TrendMicro, 2023).

Ένα παράδειγμα είναι τα βηματόμετρα που χρησιμοποιούν οι γιατροί για να παρακολουθούν τον καρδιακό ρυθμό ενός ασθενούς. Η συγκεκριμένη συσκευή συλλέγει δεδομένα από το σώμα του ασθενούς, επιτρέποντας στον γιατρό να προσαρμόσει τη λειτουργία της συσκευής στις ανάγκες του ασθενούς. Σε μια παραβίαση ασφαλείας, μια

κακόβουλη οντότητα θα μπορούσε να αποκτήσει πρόσβαση στη συσκευή, να αλλάξει τις ρυθμίσεις της και να προκαλέσει σοβαρό πρόβλημα στον ασθενή (TrendMicro, 2023).

- ***Δημιουργία πολύπλοκων περιβαλλόντων***

Η αυξανόμενη διαθεσιμότητα και η ποικιλία των συσκευών IoT σήμερα επιτρέπουν τη δημιουργία πολύπλοκων συστημάτων IoT. Στο IoT, η πολυπλοκότητα αναφέρεται σε πολλές συσκευές IoT σε ένα συγκεκριμένο περιβάλλον, επιτρέποντας δυναμικές αλληλεπιδράσεις μεταξύ τους. Αυτή η πολυπλοκότητα ενισχύει τις δυνατότητες ενός περιβάλλοντος IoT, αλλά συνοδεύεται επίσης από το κόστος της αυξημένης επιφάνειας επίθεσης (TrendMicro, 2023).

- ***Κεντροποίηση Αρχιτεκτονικών***

Η κεντροποιημένη αρχιτεκτονική αναφέρεται στα δεδομένα που συλλέγονται από κάθε συσκευή IoT και αισθητήρα που μεταφέρονται σε ένα κεντρικό σύστημα. Για παράδειγμα, ένας οργανισμός μπορεί να έχει μια κεντρική βάση δεδομένων όπου αποθηκεύονται όλα τα δεδομένα που χρησιμοποιούνται από όλες τις συσκευές IoT. Αν και αυτό μπορεί να είναι λιγότερο δαπανηρό από ένα αποκεντρωμένο σύστημα με πολλές βάσεις δεδομένων, παρέχει μεγαλύτερη επιφάνεια επίθεσης για έναν κακόβουλο χρήστη, καθώς όλες οι συσκευές επικοινωνούν με ένα κεντρικό σύστημα (TrendMicro, 2023).

Ο OWASP έχει δημιουργήσει μια λίστα με επιφάνειες επίθεσης και ευπάθειες εφαρμογών που υπάρχουν στο IoT, μαζί με πιθανές απειλές και ευαισθησίες (OWASP Foundation, 2023):

1. ***Κωδικοί ασφαλείας:*** Η χρήση διαπιστευτηρίων ελέγχου ταυτότητας εύκολα εξαναγκασμένων, κοινώς διαθέσιμων, συμπεριλαμβανομένων των backdoors σε υλικολογισμικό ή λογισμικό, μπορεί να δώσει μη εξουσιοδοτημένη πρόσβαση σε έναν εισβολέα.
2. ***Υπηρεσίες δικτύου:*** Δεν πρέπει να εκτελούνται ακατάλληλες ή ανασφαλείς υπηρεσίες δικτύου σε μια συσκευή, ειδικά εάν είναι συνδεδεμένη στο Διαδίκτυο. Αυτό μπορεί να επηρεάσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριών ή ακόμη και να επιτρέψει τον απομακρυσμένο έλεγχο από κακόβουλους χρήστες.
3. ***Διεπαφές Οικοσυστήματος:*** Μη ασφαλή web και backend API, cloud ή φορητές διεπαφές εκτός μιας συσκευής μπορεί να θέσουν σε κίνδυνο τη συσκευή ή ορισμένα

σχετικά συνδεδεμένα στοιχεία. Οι συνήθεις αιτίες περιλαμβάνουν την έλλειψη ελέγχου ταυτότητας χρήστη, την αδύναμη ή ανεπαρκή κρυπτογράφηση και την έλλειψη φιλτραρίσματος εισόδου και εξόδου.

4. ***Μηχανισμοί Ενημερώσεων:*** Αυτό σχετίζεται με την έλλειψη δυνατότητας ενημέρωσης του λογισμικού ή του υλικολογισμικού μιας συσκευής. Περιλαμβάνει την απουσία μηχανισμών επικύρωσης υλικολογισμικού, την έλλειψη ασφαλούς παράδοσης ενημερώσεων, την απουσία μηχανισμών κατά της επαναφοράς και την έλλειψη ενημερώσεων που σχετίζονται με αλλαγές ασφαλείας λόγω ενημερώσεων.
5. ***Χρήση Στοιχείων:*** Η χρήση απαρχαιωμένων ή μη ασφαλών στοιχείων λογισμικού, όπως βιβλιοθήκες, μπορεί να θέσει μια συσκευή σε κίνδυνο. Αυτό περιλαμβάνει την έλλειψη ασφαλούς διαμόρφωσης των λειτουργικών συστημάτων και τη χρήση λογισμικού ή υλικού τρίτων κατασκευαστών από μη ασφαλή μέρη της αλυσίδας εφοδιασμού.
6. ***Προστασία Ιδιωτικότητας:*** Προσωπικά στοιχεία χρηστών αποθηκευμένα στη συσκευή ή στο ευρύτερο σύστημα τα οποία χρησιμοποιούνται με μη ασφαλή ,μη ενδεδειγμένο τρόπο ή χωρίς άδεια.
7. ***Μεταφορά & Αποθήκευση Δεδομένων:*** Έλλειψη κρυπτογράφησης ή ελέγχου πρόσβασης ευαίσθητων δεδομένων σε οποιοδήποτε σημείο του οικοσυστήματος.
8. ***Διαχείριση Συσκευών:*** Έλλειψη υποστήριξης σε συσκευές που βρίσκονται εν χρήση. Περιλαμβάνει διαχείριση ενημερώσεων, ασφαλή αφαίρεση από το σύστημα, επίβλεψη της συσκευής και δυνατότητες απόκρισης.
9. ***Ρυθμίσεις Συστημάτων:*** Συσκευές ή συστήματα που διαθέτουν μη ασφαλείς εργοστασιακές ρυθμίσεις ή δεν επιτρέπουν βελτιώσεις ασφαλείας, καθώς οι χρήστες δεν επιτρέπεται να τροποποιούν τις ρυθμίσεις τους.
10. ***Φυσική Προστασία:*** Η ανεπαρκής φυσική προστασία μπορεί να επιτρέψει σε έναν εισβολέα να αποκτήσει φυσική πρόσβαση σε μια συσκευή και να εξάγει ευαίσθητες πληροφορίες από αυτήν, κάτι που θα μπορούσε να βοηθήσει σε μια μελλοντική απομακρυσμένη επίθεση ή ακόμη και να επιτρέψει τον πλήρη έλεγχο της συσκευής.

ΚΕΦΑΛΑΙΟ 4. ΜΕΤΡΑ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΕΙΛΩΝ

4.1 Ransomware and Malware

Για να ελαχιστοποιηθεί ο κίνδυνος μόλυνσης από ransomware και malware, συνιστώνται τέσσερις τρόποι δράσης:

- ***Ασφάλεια συστημάτων και δικτύων.***

Οι επιθέσεις κακόβουλου λογισμικού είναι επιτυχείς όταν οι εισβολείς εκμεταλλεύονται ευπάθειες σε λειτουργικά συστήματα, υπηρεσίες και εφαρμογές. Επομένως, η σκλήρυνση του συστήματος είναι ένας σημαντικός παράγοντας για την πρόληψη τέτοιων επιθέσεων. Παρακάτω βλέπουμε ορισμένες σημαντικές ενέργειες που μπορούν να γίνουν (Souppaya & Scarfone, 2013· CIS, 2019· Papez & Shields, 2021):

1. **Αναγνώριση διαφόρων τακτικών απειλών και τάσεων**: Συνεχείς ενημέρωση μέσω σεμιναρίων και αναφορών παρατηρητηρίων κυβερνοασφάλειας.
2. **Χρήση antivirus και anti-spam λύσεων**: Συχνές σαρώσεις συστημάτων και δικτύων για την αυτόματη ανανέωση ψηφιακών υπογραφών. Χρήση anti-spam λύσεων για το φιλτράρισμα phishing email.
3. **Ανάλυση πολλαπλών στοιχείων ενός email**: Έλεγχος Header, διεύθυνσης IP και σώματος του μηνύματος για κακόβουλο περιεχόμενο.
4. **Διαρκή ενημέρωση συστημάτων**: Περιλαμβάνει hardware, software, drivers, κινητά τηλέφωνα, υπηρεσίες cloud και CMS. Όλα τα επιμέρους συστήματα πρέπει να παραμένουν ενημερωμένα όσο το δυνατόν πιο τακτικά. Για λόγους αποδοτικότητας και διασφάλισης της λειτουργίας των διαφόρων υποσυστημάτων συνίσταται ένα κεντρικό σύστημα ενημερώσεων.
5. **Διαχωρισμός δικτύου και εφαρμογή προνομίων**: Κατηγοριοποίηση και διαχωρισμός δεδομένων με βάση την αξία τους. Υλοποίηση εικονικών περιβαλλόντων, καθώς και φυσικός και λογικός διαχωρισμός δικτύων και δεδομένων. Σκοπός είναι ο περιορισμός ζημίας σε περίπτωση μόλυνσης σε όσο το δυνατόν λιγότερα υποσυστήματα.
6. **«Παρακολούθηση» συνεργατών:** Όσοι έχουν απομακρυσμένη πρόσβαση στο δίκτυο μπορεί να αποτελέσουν σημείο εισαγωγής για κακόβουλο λογισμικό.

Επομένως θα πρέπει να «παρακολουθούνται» με σκοπό τη διασφάλιση ενός αντίστοιχα υψηλού επιπέδου κυβερνοασφάλειας.

7. **Δημιουργία Backup:** Χρήση συστημάτων backup για τη δημιουργία πολλαπλών ασφαλών αντίγραφων ειδικά για τα πιο κρίσιμα δεδομένα. Θα πρέπει να φυλάσσονται σε σημεία μη προσβάσιμα από το γενικό δίκτυο για τη διαφύλαξη τους από πιθανές κακόβουλες επιθέσεις. Πρέπει να εκτελούνται συχνά τεστ για το διασφαλισμό της ακεραιότητας των backup.
8. **Περιορισμός διαδικτυακής πρόσβασης:** Χρήση proxy server καθώς και ad-block software. Επίσης συχνές πηγές malware όπως τα προσωπικά email και οι σελίδες κοινωνικής δικτύωσης πρέπει να μπλοκαριστούν.
9. **Περιορισμός αυτόματης εκτέλεσης:** Απενεργοποίηση μηχανισμών αυτόματης εκτέλεσης προγραμμάτων και scripts, κυρίως σε Windows συστήματα.

- ***Αύξηση επίγνωσης των χρηστών***

Ένας από τους κύριους λόγους μόλυνσης ενός συστήματος είναι η εξαπάτηση υπαλλήλων μέσω διαφόρων τεχνικών. Για να αντιμετωπιστεί αυτό προτείνονται οι εξής λύσεις (Souppaya & Scarfone, 2013· CIS, 2019· Papez & Shields, 2021):

1. **Εκπαίδευση**: Εκπαίδευση για την αναγνώριση τεχνικών social engineering και phishing. Ενέργειες που μπορούν να εκτελούν για την αποφυγή επίθεσης, όπως το μη άνοιγμα ύποπτων mail και η μη επίσκεψη άγνωστων ιστοσελίδων.
2. **Ασφάλεια:** Μη απενεργοποίηση συστημάτων κυβερνοασφάλειας προσωπικού επιπέδου.
3. **Δομή αναφορών:** Ύπαρξη δομής αναφορών υπόπτων ενεργειών και αντικειμένων που μπορεί να χρησιμοποιηθεί από το προσωπικό

- ***Πολιτικές Οργανισμού***

Οι οργανισμοί θα πρέπει να έχουν ένα σύνολο πολιτικών για την αποφυγή επιθέσεων κακόβουλου λογισμικού. Μερικές βασικές αρχές που πρέπει να στηρίζουν αυτές τις πολιτικές περιγράφονται παρακάτω (Souppaya & Scarfone, 2013· CIS, 2019· Papez & Shields, 2021):

1. Σάρωση όλων των πολυμέσων που προέρχονται από εξωτερικά περιβάλλοντα για malware και άλλο κακόβουλο λογισμικό πριν χρησιμοποιηθούν.
2. Σάρωση των συνημμένων σε email αρχείων πριν ανοιχτούν.
3. Απαγόρευση αποστολής ή παραλαβής συγκεκριμένων τύπων αρχείων (πχ. .exe) μέσω email.
4. Περιορισμός μη απαραίτητου λογισμικού, κυρίως εφαρμογές που χρησιμοποιούνται για μεταφορά malware, π.χ. υπηρεσίες μεταφοράς αρχείων και torrents.
5. Περιορισμός χρήσης αφαιρούμενων συσκευών αποθήκευσης, κυρίως σε συστήματα με υψηλή πιθανότητα μόλυνσης όπως δημόσια διαθέσιμα τερματικά.
6. Διευκρίνιση των συστημάτων ασφαλείας για κάθε τύπο συσκευής, τις εφαρμογές που θα χρησιμοποιούνται καθώς και τις απαιτήσεις παραμετροποίησης και ενημέρωσης της συσκευής και του λογισμικού.

4.1.1 Ενέργειες μετά από Επίθεση

Εφόσον υπάρξει επιτυχής επίθεση, θα πρέπει να γίνουν κάποιες ενέργειες για τον περιορισμό τον ζημιών και την αποκατάσταση της ασφάλειας του συστήματος (Souppaya & Scarfone, 2013· CIS, 2019· Papez & Shields, 2021):

1. **Άμεση** αποσύνδεση του μολυσμένου συστήματος με σκοπό τον περιορισμό περαιτέρω μολύνσεων.
2. **Αναγνώριση των μολυσμένων δεδομένων και συστημάτων**. Για κάποιες συγκεκριμένες επιθέσεις και δεδομένα μπορεί να χρειάζεται και περεταίρω ενημέρωση τρίτων οργανισμών.
3. **Έρευνα για πιθανή αντιμετώπιση**. Εάν ο τρόπος αντιμετώπισης δεν είναι γνωστός, πρέπει να πραγματοποιηθεί η απαιτούμενη έρευνα το ταχύτερο δυνατό. Για παράδειγμα σε επιθέσεις ransomware μπορεί κανείς να κοιτάξει για decryptors σε διάφορες διαδικτυακές πηγές.
4. **Καθαρισμός και επαναφορά:** Καθαρισμός του συστήματος από το κακόβουλο λογισμικό και επαναφορά των αρχείων που τυχόν έχουν προσβληθεί από backup.
5. **Καταγγελία** της επίθεσης στην κατάλληλη κρατική αρχή.

4.2 Script-Based Attacks

4.2.1 SQL Injection

Οι επιθέσεις έγχυσης SQL προκαλούνται συνήθως όταν οι προγραμματιστές δημιουργούν δυναμικά ερωτήματα σε βάσεις δεδομένων που περιλαμβάνουν είσοδο χρήστη. Για την αποτροπή τέτοιων επιθέσεων, θα πρέπει να αποφεύγεται η χρήση δυναμικών ερωτημάτων στη βάση δεδομένων ή να αποτρέπεται η εκτέλεση κακόβουλων στοιχείων SQL. Υπάρχουν διάφορες διαθέσιμες τεχνικές για την αποτροπή τέτοιων απειλών, οι οποίες μπορούν να χρησιμοποιηθούν σε συνδυασμό με οποιαδήποτε γλώσσα προγραμματισμού.

Για τον μετριασμό τέτοιων απειλών, είναι σημαντικό να ακολουθείτε ορισμένες αρχές όπως η επικύρωση εισόδου, οι προετοιμασμένες δηλώσεις και τα παραμετροποιημένα ερωτήματα. Η επικύρωση εισόδου αναφέρεται στη διαδικασία επικύρωσης της εισόδου χρήστη πριν χρησιμοποιηθεί σε ένα ερώτημα, διασφαλίζοντας έτσι ότι γίνεται αποδεκτή μόνο η έγκυρη είσοδος. Οι προετοιμασμένες δηλώσεις περιλαμβάνουν την εκ των προτέρων μεταγλώττιση εντολών SQL και στη συνέχεια τη χρήση τους πολλές φορές με διαφορετικές παραμέτρους, μειώνοντας τον κίνδυνο επιθέσεων SQL injection. Τα παραμετροποιημένα ερωτήματα επιτρέπουν τη χρήση παραμέτρων εισόδου σε δηλώσεις SQL, χωρίς να τις συμπεριλαμβάνουν στο ίδιο το ερώτημα, μειώνοντας έτσι τον κίνδυνο επιθέσεων SQL injection. Αυτές οι τεχνικές μπορούν να εφαρμοστούν σε συνδυασμό με οποιαδήποτε γλώσσα προγραμματισμού για την πρόληψη επιθέσεων SQL injection (Klein, 2021・OWASP Cheat Sheet Series, 2023):

- ***Input Validation:*** Διάφορα μέρη ενός ερωτήματος SQL δεν είναι ασφαλή για τη χρήση μεταβλητών σύνδεσης, όπως ονόματα πινάκων και στηλών και μεταβλητές ταξινόμησης (ASC ή DESC). Σε αυτές τις περιπτώσεις, η καταλληλότερη άμυνα είναι η επικύρωση των δεδομένων εισόδου. Για αυτές τις μεταβλητές, οι τιμές τους πρέπει να προέρχονται από τον κώδικα και όχι από τον χρήστη.
- ***Character Escapeing:*** Ειδικοί χαρακτήρες όπως "/", "-" και ";" ερμηνεύονται από την SQL ως στοιχεία σύνταξης γλώσσας και μπορούν να χρησιμοποιηθούν για επιθέσεις SQLi όταν προστίθενται στα εισαγόμενα δεδομένα. Η προρύθμιση των δεδομένων εισόδου λέει στην SQL ποιες μεταβλητές πρέπει να χρησιμοποιηθούν ως συμβολοσειρές και ποιες ως εντολές.

- ***Minimizing Privileges:*** Για να μειωθεί η πιθανή ζημιά από επιθέσεις SQLi, θα πρέπει να υπάρχει σωστή κατανομή των δικαιωμάτων μεταξύ λογαριασμών που έχουν πρόσβαση στη βάση δεδομένων. Δεν πρέπει να παρέχονται δικαιώματα διαχειριστή σε λογαριασμούς χρηστών και η πρόσβαση των χρηστών θα πρέπει να περιορίζεται σύμφωνα με τις ενότητες της βάσης δεδομένων στις οποίες κάποιος πρέπει να έχει πρόσβαση.
- ***Vulnerability Scanners***: Μερικές φορές, είναι απαραίτητο να βρείτε το σημείο επίθεσης μιας ήδη εκτελεσθείσας επίθεσης. Αυτός είναι ο λόγος για τον οποίο τα εργαλεία δοκιμής διείσδυσης, όπως το sqlpmap ανοιχτού κώδικα, χρησιμοποιούνται για τον εντοπισμό τρωτών σημείων SQLi. Φυσικά, οι δοκιμές διείσδυσης θα πρέπει να γίνονται και προληπτικά πριν από την αρχική εγκατάσταση της βάσης δεδομένων και μετά από αλλαγές στη δομή της.
- ***Web Application Firewall:*** Για προστασία ιστότοπου, απαιτείται Τείχος προστασίας εφαρμογών Ιστού (WAF). Είναι ένας τύπος τείχους προστασίας που έχει σχεδιαστεί για την προστασία σελίδων HTTP. Εφαρμόζει κανόνες σε συνομιλίες HTTP που προστατεύουν από κοινές επιθέσεις όπως XSS και SQLi.

4.2.2 XSS Attacks

Οι επιθέσεις XSS χειραγωγούν έναν ευάλωτο ιστότοπο για να επιστρέψουν κακόβουλο JavaScript στους χρήστες, επιτρέποντας στους εισβολείς να κλέψουν ταυτότητες χρηστών και να εκτελέσουν ενέργειες μέσω του προγράμματος περιήγησής τους. Μια βασική άμυνα ενάντια στις επιθέσεις XSS είναι η εφαρμογή διαφόρων κανόνων κωδικοποίησης σε ένα έγγραφο HTML. Η κωδικοποίηση είναι η διαδικασία αντικατάστασης χαρακτήρων ελέγχου HTML με τις αντίστοιχες κωδικοποιημένες τιμές τους.

Ο κύριος σκοπός αυτών των κανόνων είναι να αποτρέψουν την εισαγωγή μη αξιόπιστων/κακόβουλων δεδομένων σε ένα αρχείο HTML. Δεδομένου ότι τα αρχεία HTML έχουν πλέον προβλέψιμη και κάπως γνωστή δομή, είναι ευκολότερο να εντοπιστούν στοιχεία που έχουν εισαχθεί από τρίτους αργότερα. Οι κανόνες χωρίζονται σε δύο ομάδες, η πρώτη ομάδα αφορά επιθέσεις Reflected & Stored XSS, ενώ η δεύτερη ομάδα αφορά επιθέσεις XSS που βασίζονται σε DOM. Αυτό συμβαίνει επειδή οι επιθέσεις από την πρώτη ομάδα εκτελούνται από την πλευρά του διακομιστή, ενώ αυτές από τη δεύτερη ομάδα εκτελούνται στην πλευρά του πελάτη (OWASP Cheat Sheet Series, 2023· OWASP Cheat Sheet Series, 2023a).

4.2.2.1 Reflected & Stored XSS

Στη συνέχεια, παρουσιάζονται οι κανόνες που σχετίζεται με το reflected and stored XSS (OWASP Cheat Sheet Series, 2023· OWASP Cheat Sheet Series, 2023a):

- ***Κανόνας 0***: Ο κανόνας 0 είναι η πλήρης άρνηση της εισαγωγής μη αξιόπιστων/κακόβουλων δεδομένων σε ένα έγγραφο HTML πέρα από τις θέσεις που καθορίζονται στους κανόνες 1 έως 5. Ο λόγος για τον κανόνα 0 είναι η ύπαρξη πολλών περίεργων πλαισίων στην HTML, τα οποία δημιουργούν μια λίστα κωδικοποίησης κανόνες πολύ περίπλοκοι.
- ***Κανόνας 1***: Ο κανόνας 1 αφορά την περίπτωση που κάποιος θέλει να εισαγάγει μη αξιόπιστα δεδομένα κάπου στο σώμα ενός εγγράφου HTML. Αυτό περιλαμβάνει κανονικές ετικέτες όπως div, p, b, td, κ.λπ. Τα περισσότερα πλαίσια web έχουν μεθόδους για την κωδικοποίηση συγκεκριμένων χαρακτήρων HTML, αλλά αυτό δεν είναι αρκετό για όλα τα περιβάλλοντα HTML. Ορισμένοι χαρακτήρες πρέπει να περάσουν από την κωδικοποίηση οντοτήτων HTML για να αποφευχθεί η αλλαγή του

περιεχομένου (σενάρια, στυλ, χειριστές συμβάντων) στο εκτελέσιμο. Αυτοί οι χαρακτήρες είναι &, <, >, ", και '.

- ***Κανόνας 2***: Ο κανόνας 2 είναι για την εισαγωγή δεδομένων σε μεταβλητές HTML όπως πλάτος, όνομα και τιμή. Οι δυναμικές μεταβλητές πρέπει να περικλείονται σε " ή '. Αυτό συμβαίνει επειδή η περικλείουσα ακολουθία μπορεί να σπάσει μέσω αυτών των δύο συμβόλων, ενώ οι μη κλειστές μεταβλητές μπορούν να σπάσουν μέσω διαφόρων συμβόλων όπως %, *, +, ,, -, /, ; , >, <, =, ^, |. Φυσικά, αυτές οι δύο μεταβλητές θα πρέπει να κωδικοποιούνται σωστά. Επιπλέον, ορισμένες μεταβλητές HTML μπορούν ακόμα να χρησιμοποιηθούν για επιθέσεις ακόμη και με κωδικοποίηση, επομένως δεν πρέπει να είναι δυναμικές και πρέπει να χρησιμοποιούνται με προσοχή.
    - Το χαρακτηριστικό "href" μπορεί να χρησιμοποιηθεί για την εισαγωγή κακόβουλου κώδικα JavaScript σε ένα έγγραφο HTML χρησιμοποιώντας ένα ψευδές πρωτόκολλο όπως "javascript:".
    - Όλοι οι χειριστές συμβάντων, όπως "onclick", "onerror" και "onmouseover", μπορούν να χρησιμοποιηθούν για την εισαγωγή κώδικα JavaScript σε ένα έγγραφο HTML.
    - Το χαρακτηριστικό "src" μπορεί επίσης να χρησιμοποιηθεί για την εισαγωγή script σε ένα έγγραφο HTML, ανάλογα με το περιβάλλον.
    - Το χαρακτηριστικό "style" μπορεί να αξιοποιηθεί μέσω της εισαγωγής χαρακτήρων ως εντολών, θέτοντας σε κίνδυνο την ασφάλεια ενός εγγράφου HTML.
- ***Κανόνας 3:*** Ο κανόνας 3 αφορά JavaScript που δημιουργείται δυναμικά για σενάρια και χειριστές συμβάντων. Το μόνο ασφαλές μέρος για την εισαγωγή μη αξιόπιστων δεδομένων περικλείεται από ". Η χρήση μη αξιόπιστων δεδομένων σε οποιαδήποτε άλλη μορφή σύνταξης JavaScript είναι επικίνδυνη, καθώς η σύνταξη μπορεί εύκολα να γίνει εκτελέσιμη μέσω χαρακτήρων όπως , =, + κ.λπ. Θα πρέπει να σημειωθεί ότι ορισμένες λειτουργίες JavaScript δεν μπορούν να προστατευτούν.
- ***Κανόνας 4:*** Ο κανόνας 4 καλύπτει την εισαγωγή μη αξιόπιστων δεδομένων σε ένα αρχείο CSS. Είναι σημαντικό τα μη αξιόπιστα δεδομένα να χρησιμοποιούνται μόνο εντός μεταβλητών ιδιοτήτων και όχι σε άλλα μέρη του CSS. Η εισαγωγή δεδομένων

σε σύνθετες μεταβλητές όπως η διεύθυνση url και η συμπεριφορά θα πρέπει να αποφεύγεται. Όπως και ο προηγούμενος κανόνας, υπάρχουν ορισμένα σημεία στη σύνταξη CSS όπου τα μη αξιόπιστα δεδομένα δεν μπορούν να εισαχθούν με ασφάλεια ακόμη και αν κωδικοποιηθούν σωστά.

- ***Κανόνας 5:*** Ο κανόνας 5 αφορά την εισαγωγή μη αξιόπιστων δεδομένων στην παράμετρο GET του HTTP. Εκτός από τους αλφαριθμητικούς χαρακτήρες, όλοι οι χαρακτήρες πρέπει να κωδικοποιούνται με τιμές ASCII μικρότερες από 256. Αυτό περιλαμβάνει μη αξιόπιστα δεδομένα. Οι μη αξιόπιστες διευθύνσεις URL δεν πρέπει να επιτρέπονται επειδή δεν υπάρχει τρόπος να αποτραπεί μια επίθεση μέσω κωδικοποίησης για να αποφευχθεί η αλλαγή της διεύθυνσης URL. Όλες οι μεταβλητές πρέπει να είναι ένθετες. Οι μη ένθετες μεταβλητές μπορούν να αποκοπούν από το αρχικό ερώτημα μέσω χαρακτήρων όπως [κενό], %, *, +, ,, -, /, ;, <, =, ^, |.

4.2.2.2 Dom Based XSS Attacks

Όπως και προηγουμένως, εδώ ακολουθούν οι κανόνες του Dom Based XSS Attacks (OWASP Cheat Sheet Series, 2023· OWASP Cheat Sheet Series, 2023a):

- ***Κανόνας 1:*** Υπάρχουν διάφορες μέθοδοι για τις μεταβλητές να αναπαριστούν περιεχόμενο HTML εντός JavaScript. Αυτές οι μέθοδοι περιλαμβάνουν το υποπλαίσιο HTML μέσα σε ένα περιβάλλον εκτέλεσης. Εάν αυτές οι μέθοδοι λαμβάνουν μη αξιόπιστο περιεχόμενο, τότε είναι δυνατή μια επίθεση XSS. Για να είναι ασφαλείς οι ενημερώσεις περιεχομένου, θα πρέπει πρώτα να εφαρμοστεί η κωδικοποίηση HTML, ακολουθούμενη από την κωδικοποίηση JavaScript.
- ***Κανόνας 2:*** Το υποπλαίσιο HTML στο πλαίσιο εκτέλεσης είναι διαφορετικό από τους τυπικούς κανόνες κωδικοποίησης. Αυτό συμβαίνει επειδή η κωδικοποίηση μεταβλητών που περιέχουν HTML μέσα σε ένα περιβάλλον εμφάνισης μεταβλητής είναι απαραίτητη για τη μείωση των επιθέσεων που μπορεί να προκύψουν από μια μεταβλητή HTML ή μπορούν να χρησιμοποιήσουν πολλές μεταβλητές, οδηγώντας έτσι σε επίθεση XSS. Όταν κάποιος βρίσκεται σε περιβάλλον εκτέλεσης DOM, απαιτείται μόνο κωδικοποίηση JavaScript για μεταβλητές HTML που δεν εκτελούν κώδικα.
- ***Κανόνας 3:*** Είναι εξαιρετικά επικίνδυνο να εισαγάγετε δυναμικά δεδομένα σε κώδικα JavaScript επειδή η κωδικοποίηση JavaScript για κωδικοποιημένα δεδομένα είναι πολύ διαφορετική από άλλες κωδικοποιήσεις. Σε πολλές περιπτώσεις, οι κωδικοποιήσεις JavaScript δεν εμποδίζουν την εκτέλεση επιθέσεων εντός του πλαισίου εκτέλεσης. Επομένως, συνιστάται να αποφεύγεται η χρήση δεδομένων σε αυτό το πλαίσιο.

4.3 Threats Against Availability and Integrity

Τα αντίμετρα κατά των επιθέσεων DoS περιλαμβάνουν διάφορα μέρη ενός οργανισμού, επομένως κάθε κατάσταση πρέπει να αναλυθεί ξεχωριστά. Είναι σημαντικό να έχετε μια σαφή κατανόηση του τρόπου χειρισμού των κατάλληλων εργαλείων για την επίλυση του προβλήματος. Επομένως, η καλή κατανόηση του περιβάλλοντος είναι απαραίτητη για την ανάπτυξη ενός κατάλληλου αμυντικού μηχανισμού. Αυτά μπορεί να περιλαμβάνουν (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β):

- Επιλογές κλιμάκωσης (πάνω ή κάτω)
- Λογικές ή θεωρητικές τεχνικές
- Ανάλυση κόστους ανάλογα με την περίπτωση

Δυστυχώς, δεν υπάρχει τρόπος να αποτραπεί ένας χάκερ από το να επιχειρήσει επίθεση DoS, αλλά οι συνέπειες μιας τέτοιας επίθεσης μπορούν να μειωθούν μέσω καλού σχεδιασμού και προληπτικών ενεργειών. Ακολουθούν ορισμένες βασικές τεχνικές που είναι απαραίτητες για τη μείωση του αντίκτυπου των επιθέσεων DoS (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β):

1. ***Δημιουργία Σχεδίου Δράσης***

Κάθε ομάδα ασφαλείας θα πρέπει να έχει ένα σχέδιο για την αποτελεσματική αντιμετώπιση μιας επίθεσης. Αυτό το σχέδιο θα πρέπει να περιλαμβάνει (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β):

- Σαφείς οδηγίες για το πώς να αντιδράσετε σε περίπτωση επίθεσης.
- Πώς να διατηρήσετε τη λειτουργικότητα μεμονωμένων συστημάτων.
- Πρωτόκολλα σε περίπτωση αύξησης της έντασης της επίθεσης.
- Μια λίστα με τα απαραίτητα εργαλεία και τα κύρια συστήματα που πρέπει να προστατευτούν.

2. Ασφάλεια δικτύου υψηλού επιπέδου

Η ασφάλεια δικτύου είναι απαραίτητη για την αποτροπή τέτοιων επιθέσεων. Μια επίθεση έχει σημαντικό αντίκτυπο όταν ο εισβολέας έχει αρκετό χρόνο για να βομβαρδίσει την υποδομή με έναν τεράστιο αριθμό ερωτημάτων. Επομένως, η δυνατότητα έγκαιρης αναγνώρισης μιας επίθεσης DDoS είναι απαραίτητη για τη μείωση της ζημιάς (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β).

Υπάρχουν διάφοροι τύποι προστασίας δικτύου στους οποίους μπορεί κανείς να βασιστεί (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β):

- Τείχη προστασίας και συστήματα ανίχνευσης εισβολών για σάρωση δικτύων.
- Εργαλεία ασφαλείας Ιστού για τον αποκλεισμό ύποπτης κυκλοφορίας δικτύου.
- Διαχωρισμός του δικτύου σε υποδίκτυα ώστε να μην επηρεάζεται ολόκληρο το δίκτυο σε περίπτωση επίθεσης.

3. Επάρκεια Πόρων

Η χρήση πολλαπλών κατανεμημένων διακομιστών προτείνεται για να αυξήσει τη δυσκολία για έναν εισβολέα να στοχεύσει όλους τους διακομιστές ταυτόχρονα. Ακόμα κι αν μια επίθεση είναι επιτυχής σε έναν συγκεκριμένο διακομιστή, οι άλλοι θα παραμείνουν ανεπηρέαστοι και θα χειριστούν την πρόσθετη κίνηση μέχρι να αποκατασταθεί το σύστημα που έχει επιτεθεί. Για να αποφευχθεί η συμφόρηση δικτύου κατά τη διάρκεια μιας επίθεσης, οι διακομιστές θα πρέπει να είναι κατανεμημένοι σε διαφορετικές γεωγραφικές περιοχές και να χρησιμοποιούν διαφορετικά δίκτυα (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β).

4. Ανίχνευση Σημάτων Κινδύνου

Η ομάδα ασφαλείας θα πρέπει να είναι σε θέση να ανιχνεύει σημάδια επίθεσης προκειμένου να ελαχιστοποιήσει τη ζημιά. Τα πιο κοινά σημάδια περιλαμβάνουν (Velimirovic, 2023 • OWASP Cheat Sheet Series, 2023β):

- Χαμηλή συνδεσιμότητα
- Αργή απόδοση
- Υψηλή ζήτηση για συγκεκριμένο πόρο
- Διακοπή λειτουργίας ορισμένων συστημάτων
- Ασυνήθιστος όγκος κίνησης που προέρχεται από μια συγκεκριμένη διεύθυνση IP.

4.4 Threats against Data

4.4.1 Man in the Middle

Οι επιθέσεις man-in-the-middle επιτρέπουν στους εισβολείς να κρυφακούουν ή να τροποποιούν κυρίως ασύρματες επικοινωνίες. Για τον μετριασμό των κινδύνων τέτοιων επιθέσεων και τη μείωση της απειλής, πρέπει να ακολουθηθούν συγκεκριμένες στρατηγικές (Snyder, 2022):

- ***Κρυπτογράφηση***: Όλα τα σύνολα δεδομένων των εφαρμογών που χρησιμοποιούνται θα πρέπει να είναι κρυπτογραφημένα και όχι μόνο οι ροές δεδομένων που μεταφέρουν ευαίσθητα δεδομένα. Εάν ένας εισβολέας αποκτήσει πρόσβαση σε μία ροή δεδομένων, μπορεί να εισαγάγει δεδομένα που μπορεί να του επιτρέψουν να αποκτήσει πρόσβαση σε άλλες ροές, ακόμη και σε αυτές που είναι κρυπτογραφημένες. Μια λύση είναι να χρησιμοποιήσετε το πρότυπο HTTPS-Only και HTTP Strict Transport Security που δεν επιτρέπουν στις εφαρμογές να χρησιμοποιούν μη κρυπτογραφημένες μεθόδους επικοινωνίας στην υποδομή του οργανισμού. Όσον αφορά τις κινητές συσκευές, μπορούν να ρυθμιστούν ώστε να χρησιμοποιούν VPN για κάθε επικοινωνία, στέλνοντας όλη την κίνηση σε ένα κέντρο δεδομένων του οργανισμού ή στον πάροχο υπηρεσιών VPN (Snyder, 2022).
- ***TLS/SSL***: Πολλοί διακομιστές Ιστού στις αρχικές τους ρυθμίσεις επιτρέπουν τη χρήση παλαιότερων πρωτοκόλλων ασφαλείας και ασθενέστερων αλγορίθμων κρυπτογράφησης και ελέγχου ταυτότητας, τους οποίους μπορούν να εκμεταλλευτούν οι εισβολείς. Επομένως, είναι καλή πρακτική να απενεργοποιείτε παλαιότερους και πιο ευάλωτους αλγόριθμους ασφαλείας. Είναι απαραίτητο να υπάρχει ένας κεντρικός τρόπος διαχείρισης των ρυθμίσεων TLS/SSL, που είναι τα κυρίαρχα πρωτόκολλα σε αυτόν τον τομέα, καθώς και για τη συνεχή ενημέρωση των βιβλιοθηκών σε νεότερες εκδόσεις (Snyder, 2022).
- ***Ψηφιακά πιστοποιητικά σε ολόκληρο τον οργανισμό***: Μόνο έγκυρα ψηφιακά πιστοποιητικά θα πρέπει να χρησιμοποιούνται στις εφαρμογές ενός οργανισμού. Εάν ένας οργανισμός χρησιμοποιεί τα πιστοποιητικά του, θα πρέπει να είναι προφορτωμένα σε όλες τις συσκευές. Επίσης, η δυνατότητα ανάκλησης πιστοποιητικού εξ αποστάσεως θα πρέπει να είναι ενεργή (Snyder, 2022).

4.5 Non-Malicious Threats

Η αμέλεια του προσωπικού είναι μια κύρια αιτία κενών ασφαλείας, τα οποία μπορούν να αξιοποιηθούν για οποιαδήποτε επίθεση. Για να αποφευχθεί αυτό, θα πρέπει να ληφθούν μια σειρά από ενέργειες (ENISA, 2021):

- Υιοθέτηση μιας διαδικασίας διαχείρισης κινδύνου που περιλαμβάνει μη κακόβουλες απειλές.
- Αποφυγή της λεγόμενης σκιώδης πληροφορικής, δηλαδή ανάπτυξη έργων και συστημάτων πληροφορικής χωρίς τη γνώση του τμήματος Πληροφορικής.
- Συνεχής παρακολούθηση και έλεγχος για τον εντοπισμό σφαλμάτων και κακής διαχείρισης.
- Κατάλληλες πολιτικές ασφαλείας για τη μείωση του ανθρώπινου λάθους.
- Σχέδιο διαχείρισης ενημερώσεων για αποτελεσματική εκτέλεση ενημερώσεων, όπου χρειάζεται, μέσω διαδικασιών διαχείρισης κινδύνου.
- Επικοινωνία με κατασκευαστές για δημιουργία ενημερώσεων σε περιπτώσεις ανεπάρκειας και αδυναμίας κάλυψης τρωτών σημείων.
- Η διαχείριση των ενημερώσεων θα πρέπει να λαμβάνει υπόψη τις επιθέσεις στην αλυσίδα εφοδιασμού.
- Οι ενημερώσεις θα πρέπει να εκτελούνται με ασφαλή τρόπο.
- Εκπαίδευση προσωπικού σε θέματα κυβερνοασφάλειας, με στόχο την πρόληψη λαθών λόγω έλλειψης γνώσεων. Ιδιαίτερη προσοχή πρέπει να δοθεί στα ανώτερα στελέχη που χειρίζονται ευαίσθητα δεδομένα.
- Η κατασκευή φυσικών εγκαταστάσεων θα πρέπει να είναι ανθεκτική σε φυσικές καταστροφές. Η διαχείρισή τους θα πρέπει να λαμβάνει υπόψη απροσδόκητες καταστάσεις.
- Σχέδια ανάκτησης δεδομένων και δημιουργίας αντιγράφων ασφαλείας για την ανθεκτικότητα των συστημάτων.
- Φυσική ασφάλεια συσκευών. Η πρόσβαση ενός εισβολέα σε μια φυσική συσκευή είναι ένας από τους τρόπους που μπορεί να προκαλέσει το μέγιστο ποσό ζημιάς.

4.6 Disinformation - Misinformation

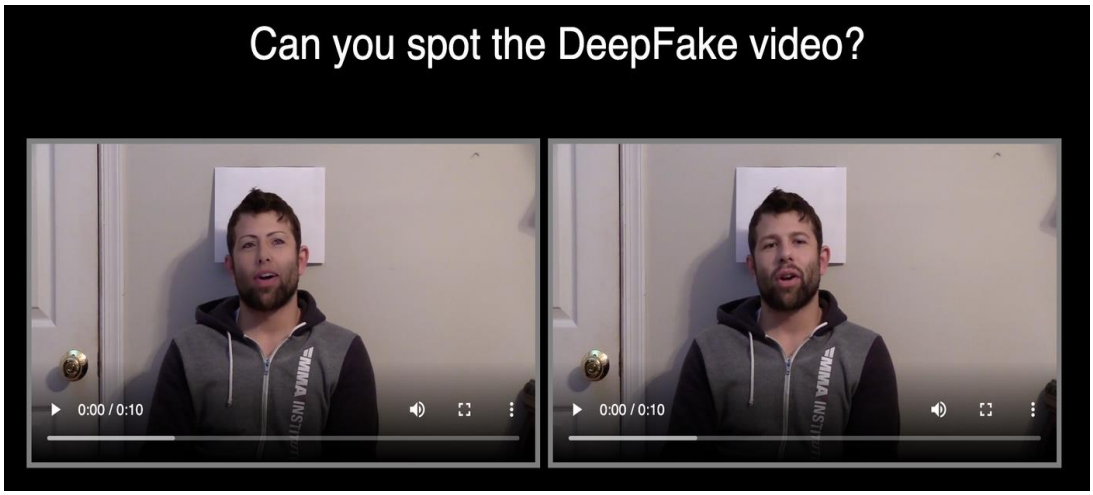
Η διάκριση μεταξύ ενός πραγματικού βίντεο και ενός deepfake είναι αρκετά προκλητική, ειδικά τα τελευταία χρόνια όπου χρησιμοποιούνται τεχνολογίες AI, καθιστώντας τη διάκριση όλο και πιο δύσκολη. Αυτό συμβαίνει επειδή χρησιμοποιούνται τεχνολογίες μηχανικής μάθησης για τη δημιουργία μιας όσο το δυνατόν πιο ρεαλιστικής προσομοίωσης. Ωστόσο, οι δυσκολίες που προκύπτουν δεν είναι ανυπέρβλητες, καθώς υπάρχουν σχεδόν πάντα μέθοδοι που μπορεί κανείς να χρησιμοποιήσει για να διακρίνει ένα deepfake, δεδομένου ότι οι παρούσες τεχνικές δεν μπορούν να προσομοιώσουν πλήρως τα φυσικά φαινόμενα.

Εκμεταλλευόμενος αυτή την προαναφερθείσα αδυναμία, μπορεί κανείς να αναζητήσει συγκεκριμένες ατέλειες που βοηθούν στη διάκριση ενός deepfake. Δεδομένου ότι η πλειοψηφία των deepfakes είναι σχεδόν πάντα προσομοιώσεις προσώπου, θα πρέπει να δοθεί ιδιαίτερη προσοχή στο πρόσωπο του ατόμου που απεικονίζεται στο βίντεο. Αυτό που πρέπει να παρατηρήσει κανείς είναι (MIT Media Lab, 2023):

- Τα μάγουλα και το μέτωπο του ατόμου είναι επιρρεπή σε αρκετές επεμβάσεις. Είναι το δέρμα πολύ λείο ή πολύ ζαρωμένο; Η γήρανση του δέρματος μοιάζει με τη γήρανση των μαλλιών και των ματιών ή όχι;
- Ειδικά στα μάτια και τις βλεφαρίδες θα πρέπει να παρατηρήσει κανείς αν υπάρχουν σκιές εκεί που πρέπει.
- Ιδιαίτερη προσοχή δίνεται στα γυάλινα αντικείμενα. Υπάρχει υποψία προβληματισμού; Υπάρχει έντονη λάμψη; Αλλάζει η γωνία ανάκλασης όταν υπάρχει κίνηση;
- Ένα εξίσου σημαντικό σημείο του προσώπου που πρέπει να προσέξετε είναι η παρουσία μικρού ή μεγάλου γένιου, κάθε είδους μουστάκι ή η απουσία τους. Αν υπάρχουν, ανταποκρίνονται στην πραγματικότητα; Αν δεν υπάρχουν, είναι φυσικό το δέρμα;
- Ιδιαίτερη προσοχή πρέπει να δοθεί στα σπυράκια που εμφανίζονται συχνά στο δέρμα του προσώπου. Φαίνονται αληθινά;
- Η κίνηση των βλεφάρων αξίζει ιδιαίτερης αναφοράς. Αναβοσβήνουν σε τακτά χρονικά διαστήματα ή συνέχεια;

- Τέλος, θα πρέπει να δοθεί προσοχή στο μέγεθος και το χρώμα των χειλιών του ατόμου. Ταιριάζουν ή είναι εντελώς αταίριαστα με το υπόλοιπο πρόσωπο του ατόμου;

Εικόνα 22. Παράδειγμα deepfake, April 21, 2023, https://www.media.mit.edu/projects/detect-fakes/overview/



Στην παραπάνω εικόνα βλέπουμε ένα παράδειγμα Deepfake. Η αριστερή εικόνα είναι η ψεύτικη και αυτό μπορεί κάνεις να το διακρίνει κανείς από τον τόνο του χρώματος του δέρματος.

Εικόνα 23. Jonathan Hui, 2020: Παράδειγμα deepfake, April 21, 2023, <https://jonathan-hui.medium.com/detect-ai-generated-images-deepfakes-part-1-b518ed5075f4>

Εδώ πάλι βλέπουμε μια ψεύτικη εικόνα που έχει δημιουργηθεί από ένα A.I. Παρατηρώντας την κλήση των ώμων μπορούμε να καταλάβουμε ότι είναι ψεύτικη, μιας και η κλήση του δεξιού ομού είναι αρκετά απότομη σε σχέση με τον αριστερό.

4.7 Advanced Persistent Threats

Ο εντοπισμός και η προστασία από προχωρημένες επίμονες απειλές (APT) απαιτούν μια σειρά μέτρων που πρέπει να λάβει ένας οργανισμός.

- ***Traffic Monitoring***

Μία από τις βέλτιστες πρακτικές για την αποτροπή της εγκατάστασης κερκόπορτων και της επακόλουθης διείσδυσης ευαίσθητων δεδομένων είναι η παρακολούθηση της κυκλοφορίας. Παρακολουθώντας τις ροές δεδομένων σε μια περίμετρο δικτύου, μπορεί κανείς να παρατηρήσει ανωμαλίες που μπορεί να υποδηλώνουν κάποιο είδος επίθεσης. Ένα τείχος προστασίας διαδικτυακών εφαρμογών (WAF), το οποίο έχει ρυθμιστεί στην περίμετρο του δικτύου, φιλτράρει τις ροές δεδομένων προς διακομιστές εφαρμογών Ιστού, προστατεύοντας έτσι ένα από τα πιο ευάλωτα σημεία του συστήματος ενός οργανισμού. Ένα WAF μπορεί να αποτρέψει κοινές επιθέσεις σε επίπεδο εφαρμογής, όπως η έγχυση SQL. Στην εσωτερική πλευρά του δικτύου, υπηρεσίες όπως τα τείχη προστασίας δικτύου χρησιμοποιούνται για τον εντοπισμό ροών δεδομένων. Παρέχουν μια άποψη των αλληλεπιδράσεων μεταξύ των χρηστών μέσα στο δίκτυο, βοηθώντας έτσι στον εντοπισμό ανωμαλιών όπως οι ασυνήθιστες μεταφορές δεδομένων μεγάλου όγκου. Τέτοιες ενέργειες μπορεί να υποδηλώνουν επίθεση APT (Learning Center, 2023b· Crowdstrike, 2023).

- ***Application and Domain Whitelisting***

Η επιτρεπόμενη λίστα είναι μια μέθοδος ελέγχου της προσβασιμότητας του τομέα και των εφαρμογών που μπορούν να εγκατασταθούν στους υπολογιστές ενός οργανισμού. Είναι μια άλλη τεχνική για την ελαχιστοποίηση της επιτυχίας μιας επίθεσης APT. Ομοίως, οι τεχνικές μαύρης λίστας μπορούν επίσης να χρησιμοποιηθούν για τον αποκλεισμό της πρόσβασης σε ορισμένους ιστότοπους που είναι γνωστό ότι έχουν αυξημένο κίνδυνο μόλυνσης. Ωστόσο, δεν είναι μια αλάνθαστη μέθοδος, καθώς ακόμη και οι πιο αξιόπιστοι τομείς και εφαρμογές

μπορούν να μολυνθούν με κακόβουλο λογισμικό. Είναι επίσης γνωστό ότι τα κακόβουλα αρχεία συνήθως αποτελούν μέρος αξιόπιστου λογισμικού. Επιπλέον, οι παλαιότερες εκδόσεις του λογισμικού είναι συνήθως πιο ευάλωτες σε κακόβουλες επιθέσεις. Η αποτελεσματική προσθήκη στη λίστα επιτρεπόμενων απαιτεί αυστηρές πολιτικές ενημέρωσης της έκδοσης λογισμικού για να διασφαλιστεί ότι είναι πάντα στην καλύτερη δυνατή κατάσταση (Κέντρο Μάθησης, 2023b· Crowdstrike, 2023).

- ***Access Control***

Οι εργαζόμενοι είναι συχνά η μεγαλύτερη και πιο κοινή αδυναμία ενός οργανισμού, καθιστώντας τους ένα εύκολο σημείο εισόδου για τους επιτιθέμενους. Συνήθως, οι εργαζόμενοι μπορούν να κατηγοριοποιηθούν σε τρεις κατηγορίες (Learning Center, 2023b· Crowdstrike, 2023):

1. Αφελείς χρήστες που δεν γνωρίζουν τις πολιτικές ασφαλείας και δίνουν άθελά τους πρόσβαση σε εισβολείς.
2. Κακόβουλοι μυστικοί που καταχρώνται τα προνόμιά τους για να παραχωρήσουν πρόσβαση σε εισβολείς.
3. Χρήστες των οποίων οι λογαριασμοί έχουν παραβιαστεί.

Η δημιουργία αποτελεσματικού ελέγχου πρόσβασης απαιτεί πλήρη κατανόηση του προσωπικού ενός οργανισμού και των πληροφοριών στις οποίες έχει πρόσβαση. Για παράδειγμα, η κατηγοριοποίηση των δεδομένων ως εμπιστευτικών μπορεί να εμποδίσει την ικανότητα του εισβολέα να προβάλλει αρχεία μέσω ενός λογαριασμού υπαλλήλου χαμηλού επιπέδου.

Οι σύγχρονες βέλτιστες πρακτικές παροτρύνουν τους διαχειριστές συστημάτων να εξασφαλίσουν την πρόσβαση σε κρίσιμα συστήματα με έλεγχο ταυτότητας δύο παραγόντων. Αυτή η πολιτική απαιτεί από τον υπάλληλο να χρησιμοποιεί έναν δεύτερο τύπο ελέγχου ταυτότητας πέρα από τον αρχικό κωδικό πρόσβασής του, καθιστώντας την πρόσβαση πιο δύσκολη για τους εισβολείς, καθώς θα έπρεπε να αποκτήσουν δύο μορφές "πιστοποιητικών" (Learning Center, 2023b· Crowdstrike, 2023).

Επίσης υπάρχουν και άλλες ενέργειες που μπορούν να γίνουν όπως (Learning Center, 2023b· Crowdstrike, 2023):

- Κρυπτογράφηση απομακρυσμένων συνδέσεων.
- Φιλτράρισμα email για αποφυγή spam και phising.
- Πλήρης καταγραφή συμβάντων ασφαλείας για τη βελτίωση πολιτικών ασφαλείας και whitelisting.

4.8 Internet-of-Things

Όπως αναφέρθηκε στο προηγούμενο κεφάλαιο, όλα τα απαραίτητα συστήματα IoT μπορούν να γίνουν περιοχές επίθεσης. Ως εκ τούτου, η ασφάλεια θα πρέπει να αποτελεί προτεραιότητα στο σχεδιασμό και τη συντήρηση των συστημάτων IoT. Ανεξάρτητα από το μέγεθος και τον τύπο του περιβάλλοντος στο οποίο αναπτύσσεται ένα σύστημα IoT, η ασφάλεια θα πρέπει να λαμβάνεται υπόψη από τη φάση του σχεδιασμού ώστε να ενσωματώνεται καλύτερα σε κάθε μέρος του συστήματος. Με αυτόν τον τρόπο, οι ρυθμίσεις συστήματος, είτε σε επίπεδο συσκευής είτε σε επίπεδο ολόκληρου συστήματος, μπορούν να είναι λειτουργικές και ασφαλείς (Coudflare, 2023; TrendMicro, 2023).

Για το λόγο αυτό, υπάρχουν ορισμένες κατευθυντήριες γραμμές που πρέπει να ληφθούν υπόψη (Coudflare, 2023; TrendMicro, 2023):

- ***Όλα τα δεδομένα που συλλέγονται και οι πληροφορίες που αποθηκεύονται πρέπει να καταγράφονται***. Κάθε κομμάτι δεδομένων και πληροφοριών που κυκλοφορεί σε ένα πιο ολοκληρωμένο σύστημα IoT θα πρέπει να χαρτογραφείται επαρκώς. Αυτό αναφέρεται σε αισθητήρες και συσκευές και στοιχεία ελέγχου ταυτότητας σε διακομιστές αυτοματισμού ή άλλες εφαρμογές IoT.
- ***Κάθε συσκευή που είναι συνδεδεμένη στο δίκτυο θα πρέπει να διαμορφώνεται με βάση την ασφάλεια.*** Το επίπεδο ασφαλείας των ρυθμίσεων μιας συσκευής θα πρέπει πάντα να επαληθεύεται προτού συνδεθεί στο δίκτυο. Αυτό περιλαμβάνει έναν ισχυρό συνδυασμό ονόματος χρήστη και κωδικού πρόσβασης, τύπων ελέγχου ταυτότητας πολλαπλών παραγόντων και κρυπτογράφηση.
- ***Η στρατηγική ασφαλείας θα πρέπει να οικοδομηθεί με βάση την υπόθεση του συμβιβασμού***. Αν και η αποφυγή μιας πιθανής επίθεσης είναι σημαντική, θα πρέπει να γίνει κατανοητό ότι δεν υπάρχει τέλεια άμυνα έναντι απειλών που εξελίσσονται συνεχώς. Επομένως, πρέπει να υπάρχουν πρωτόκολλα για τον περιορισμό και τον μετριασμό των συνεπειών μιας επίθεσης.
- ***Κάθε συσκευή πρέπει να είναι φυσικά ασφαλισμένη***. Είναι σημαντικό να λαμβάνεται υπόψη η φυσική πρόσβαση σε συσκευές IoT. Εάν μια συσκευή δεν έχει ασφαλιστεί σωστά από παρεμβολές, θα πρέπει είτε να ασφαλιστεί επαρκώς είτε να αποθηκευτεί σε περιοχή περιορισμένης πρόσβασης. Για παράδειγμα, οι κάμερες IP

μπορούν να παραβιαστούν εάν ένας κυβερνοεγκληματίας αποκτήσει πρόσβαση σε αυτές. Μπορεί να προσθέσουν ένα κομμάτι κακόβουλου υλικού ή λογισμικού που μπορεί να προκαλέσει προβλήματα στο ευρύτερο σύστημα ή να διαδώσει κακόβουλο λογισμικό.

4.9 Virtualization

Οι οργανισμοί που χρησιμοποιούν τεχνολογίες εικονικοποίησης πρέπει να εκτελούν έναν σημαντικό συνδυασμό ενεργειών για να μειώσουν τους κινδύνους που ενέχουν για την ασφάλειά τους. Το πρώτο βήμα είναι η κατηγοριοποίηση όλων των ενεργών τύπων εικονικοποίησης, καθώς και των μέτρων ασφαλείας πέρα από τις ενσωματωμένες ρυθμίσεις του hypervisor. Οι ρυθμίσεις ασφαλείας θα πρέπει να συγκρίνονται με τα πρότυπα ασφαλείας του κλάδου για να εντοπιστούν τυχόν κενά και τρόποι για να καλυφθούν το συντομότερο δυνατό. Αυτές οι ρυθμίσεις θα πρέπει να περιλαμβάνουν προστασία από ιούς, ανίχνευση εισβολής και ενεργή σάρωση ευπάθειας (Penetration Testing Lab, 2013; Atumu, 2021). Επιπλέον, θα πρέπει να ληφθούν πρόσθετα μέτρα (Penetration Testing Lab, 2013· Atumu, 2021):

- ***VM traffic monitoring:*** Η δυνατότητα παρακολούθησης της ροής δεδομένων σε μια υποδομή VM είναι απαραίτητη. Οι παραδοσιακές μέθοδοι δεν μπορούν να παρακολουθούν τις ροές δεδομένων στο ψηφιακό περιβάλλον, καθώς ελέγχονται από εικονικούς διακόπτες. Οι υπερεπόπτες διαθέτουν αποτελεσματικά εργαλεία παρακολούθησης που θα πρέπει να είναι ενεργά.
- ***Administrative Control***: Η ασφαλής πρόσβαση ενδέχεται να διακυβευτεί λόγω εξάπλωσης του VM ή άλλων λόγων. Επομένως, οι διαδικασίες ελέγχου ταυτότητας, διαχείρισης ταυτότητας και καταγραφής θα πρέπει να είναι πλήρως ασφαλείς.
- ***Customer security***: Εκτός από τα VM, θα πρέπει να υπάρχουν προστασίες για υπηρεσίες που έρχονται σε επαφή με τον πελάτη, όπως οι ιστότοποι.
- ***VM segregation***: Θα πρέπει να υπάρχει λειτουργικός διαχωρισμός των VM. Για παράδειγμα, θα πρέπει να δημιουργηθούν ξεχωριστές ζώνες για σταθμούς εργασίας, διακομιστές και δοκιμαστικούς διακομιστές. Ο σκοπός είναι να μειωθούν οι αλληλεπιδράσεις μεταξύ των VM σε διαφορετικές ζώνες στο μέγιστο απαραίτητο.
- ***Auditing Software:*** Αυτό είναι λογισμικό που ελέγχει και παρακολουθεί το ευρύτερο ψηφιακό περιβάλλον και ειδοποιεί τους διαχειριστές για πιθανές απειλές. Η χρήση του σε περιβάλλον όπου υπάρχουν VM μπορεί να οδηγήσει στην έγκαιρη διάγνωση πιθανών κινδύνων (NewsWatch, 2023).

- ***Replication Softwar:*** Λογισμικό δημιουργίας αντιγράφων ασφαλείας που επιτρέπει την κλωνοποίηση εικονικών μηχανών σε χώρο αποθήκευσης cloud. Με αυτόν τον τρόπο, εάν ένα VM πέσει θύμα επίθεσης, μπορεί κανείς εύκολα να επαναφέρει το σύστημα σε προηγούμενη, υγιή κατάσταση και να λάβει τα κατάλληλα μέτρα για να ελαχιστοποιήσει την πιθανότητα επίθεσης (NewsWatch, 2023).

ΚΕΦΑΛΑΙΟ 5. ΣΧΕΔΙΟ ΑΝΤΙΜΕΤΩΠΙΣΗΣ ΑΠΕΙΛΩΝ

Μια σημαντική πτυχή της επιτυχίας ενός οργανισμού είναι μια πολιτική ασφάλειας στον κυβερνοχώρο. Η πολιτική ασφαλείας καθορίζει την ετοιμότητα και την απόκριση ενός οργανισμού σε μια επίθεση. Θα πρέπει να προσδιορίζει ποιο προσωπικό είναι υπεύθυνο για ποιες πληροφορίες εντός του οργανισμού.

Μια ολοκληρωμένη πολιτική ασφαλείας προσφέρει πολλά πλεονεκτήματα σε έναν οργανισμό. Μπορεί να μειώσει τον αριθμό των προβλημάτων κυβερνοασφάλειας που μπορεί να προκύψουν σε έναν οργανισμό, καθώς οι εργαζόμενοι θα έχουν την πολιτική ως σημείο αναφοράς για τον τρόπο αντιμετώπισης ενός ζητήματος ασφάλειας. Μπορεί επίσης να προετοιμάσει έναν οργανισμό για ελέγχους από κυβερνητικούς φορείς διασφαλίζοντας τη συμμόρφωση με την απαραίτητη νομοθεσία.

Μια πολιτική ασφαλείας πρέπει να περιλαμβάνει το σκοπό, το πεδίο εφαρμογής, τους κανόνες και τις διαδικασίες που πρέπει να ακολουθούνται. Θα πρέπει να περιλαμβάνει κώδικες συμπεριφοράς για όλους τους εργαζόμενους, καθώς και συνέπειες για όσους δεν τους ακολουθούν. Θα πρέπει να προσαρμόζεται με βάση τις απειλές και τις ανάγκες ενός οργανισμού, παρέχοντας καθοδήγηση για την προστασία από αυτές τις απειλές.

Οι πιο σημαντικές πολιτικές επιβάλλονται σε όλους τους εργαζόμενους ενός οργανισμού. Αυτές οι πολιτικές προστατεύουν την ακεραιότητα, τη διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριακών συστημάτων και των δεδομένων ενός οργανισμού. Αυτές οι πολιτικές παρουσιάζονται στις ακόλουθες υποενότητες.

5.1 Acceptable User Policy

Η Πολιτική Αποδεκτού Χρήστη (Acceptable User Policy AUP) περιγράφει την κατάλληλη χρήση των συστημάτων πληροφοριών ενός οργανισμού. Καθορίζει περιορισμούς και πρακτικές που πρέπει να γνωρίζουν οι χρήστες προκειμένου να έχουν πρόσβαση στο δίκτυο του οργανισμού. Καθορίζει επίσης τις απαράδεκτες χρήσεις των πληροφοριακών συστημάτων και τα προβλήματα που δημιουργούν. Το AUP είναι ιδιαίτερα σημαντικό γιατί η μη συμμόρφωση με τις οδηγίες μπορεί να οδηγήσει σε κενά ασφαλείας στο δίκτυο, καθώς και σε νομικές συνέπειες. Ορισμένα παραδείγματα πολιτικών AUP παρέχονται από την SecurityScorecard (2023) και την Adsero Security (2023).

Οι χρήστες υποχρεούνται να:

- Προστατέψουν το User ID, την ψηφιακή υπογραφή και τον κωδικό πρόσβασής τους από μη εξουσιοδοτημένη χρήση. Κάθε χρήστης είναι υπεύθυνος για οποιαδήποτε πρόσβαση στα συστήματα του οργανισμού που γίνεται με βάση το User ID του (University IT, 2021).
- Ασφαλίσουν τα συστήματά τους με κωδικούς πρόσβασης που συμμορφώνονται με τις προδιαγραφές της πολιτικής ασφαλείας για κωδικούς πρόσβασης (Information Technology, 2021).
- Παρέχουν πρόσβαση μόνο σε πληροφορίες που έχουν εξουσιοδοτηθεί ή είναι δημόσια προσβάσιμες (University IT, 2021).
- Προστατέψουν τα δεδομένα που κατηγοριοποιούνται ως υψηλού επιπέδου.
- Κρυπτογραφούν τα δεδομένα σύμφωνα με την πολιτική κρυπτογράφησης του οργανισμού (Information Technology, 2021).
- Χρησιμοποιούν νόμιμα λογισμικό που προστατεύεται από πνευματικά δικαιώματα (University IT, 2021).
- Αποφύγουν τη σπατάλη κοινόχρηστων πόρων, όπως υπερφόρτωση δικτύου, εκτύπωση χαρτιού, ψηφιακό αποθηκευτικό χώρο κ.λπ. (University IT, 2021).
- Να είναι προσεκτικοί όταν ανοίγετε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς, καθώς ενδέχεται να περιέχουν κακόβουλο λογισμικό (Information Technology, 2021).

- Αποθηκεύουν εμπιστευτικά δεδομένα μόνο σε εγκεκριμένες ασφαλείς τοποθεσίες (University IT, 2021).
- Μεταφέρουν δεδομένα και πληροφορίες μόνο μέσω εγκεκριμένων ασφαλών μέσων (University IT, 2021).
- Αλλάζουν τα μέσα ελέγχου ταυτότητας χρήστη σε περίπτωση υποψίας παραβίασης (University IT, 2021).

Οι ακόλουθες είναι απαγορευμένες ενέργειες βάσει της Πολιτικής Αποδεκτών Χρηστών:

- Οι χρήστες δεν πρέπει να αποκτούν πρόσβαση ή να χρησιμοποιούν το σύστημα, τα αρχεία ή τα δεδομένα συναδέλφων τους χωρίς την άδειά τους (University IT, 2021).
- Οι χρήστες δεν πρέπει να αποκαλύπτουν κωδικούς πρόσβασης ή οποιοδήποτε άλλο μέσο ελέγχου ταυτότητας σε οποιοδήποτε άλλο πρόσωπο (University IT, 2021).
- Οι χρήστες δεν πρέπει να χρησιμοποιούν προγράμματα αποκρυπτογράφησης κωδικού πρόσβασης ή άλλα μέσα ελέγχου ταυτότητας (University IT, 2021).
- Οι χρήστες δεν πρέπει να χρησιμοποιούν προγράμματα ή τεχνικές για την παρακολούθηση δεδομένων στο δίκτυο του οργανισμού (Information Technology, 2021).
- Οι χρήστες δεν πρέπει να επιχειρούν να παρακάμψουν συστήματα ασφαλείας για κανένα λόγο.
- Οι χρήστες δεν πρέπει να χρησιμοποιούν παράνομο λογισμικό (University IT, 2021).
- Οι χρήστες δεν πρέπει να στέλνουν ή να λαμβάνουν εμπιστευτικές πληροφορίες χωρίς τις απαραίτητες ρυθμίσεις ασφαλείας (University IT, 2021).
- Οι χρήστες δεν πρέπει να τροποποιούν τα δεδομένα του οργανισμού χωρίς άδεια.
- Οι χρήστες δεν πρέπει να προβαίνουν σε καμία ενέργεια που θα μπορούσε να προκαλέσει σκόπιμα βλάβη στα συστήματα του οργανισμού (University IT, 2021).
- Οι χρήστες δεν πρέπει να εμπλέκονται σε οποιοδήποτε είδος κακόβουλης δραστηριότητας χρησιμοποιώντας τα συστήματα του οργανισμού, όπως η εξαπάτηση ατόμων χρησιμοποιώντας το email του οργανισμού ως μέσο επικοινωνίας (Information Technology, 2021).

5.2 Security Awareness and Training

Το Security Awareness and Training είναι μια στρατηγική που χρησιμοποιείται από τα τμήματα τεχνολογίας πληροφοριών για τη μείωση ή την πρόληψη προβλημάτων που προκαλούνται από τους χρήστες. Αυτά τα προγράμματα έχουν σχεδιαστεί για να βοηθούν τους χρήστες να κατανοούν διάφορες απειλές στον κυβερνοχώρο, πώς να αναγνωρίζουν και να προστατεύονται από αυτές και τον ρόλο τους στην ασφάλεια ενός οργανισμού. Αυτή η εκπαίδευση βοηθά στη μείωση των σφαλμάτων που θα μπορούσαν να οδηγήσουν σε κλοπή πνευματικής ιδιοκτησίας και ιδιοκτησιακών πληροφοριών και χρημάτων, καθώς και σε βλάβη της φήμης ενός οργανισμού. Ένα αποτελεσματικό πρόγραμμα εστιάζει σε λάθη που γίνονται μέσω email και ιστοσελίδων, καθώς και σε λάθη που αφορούν φυσικά μέσα, όπως USB sticks, μεταξύ άλλων. Επομένως, ένα καλό πρόγραμμα εκπαίδευσης θα πρέπει να περιλαμβάνει τα ακόλουθα θέματα (Mimecast, 2023 • Curricula, 2012):

- ***Phishing awareness:*** διδασκαλία στους χρήστες πώς να αναγνωρίζουν και να χειρίζονται επιθέσεις phishing.
- ***Password Security:*** οδηγίες για τη δημιουργία ισχυρών κωδικών πρόσβασης. Οι χρήστες θα πρέπει να ενθαρρύνονται να αποφεύγουν τη χρήση κωδικών πρόσβασης που προέρχονται από προσωπικές πληροφορίες, εξηγώντας πόσο ευάλωτοι είναι σε τεχνικές κοινωνικής μηχανικής.
- ***Απόρρητο:*** οδηγίες για την προστασία των προσωπικών δεδομένων συναδέλφων και πελατών.
- ***Legal Compliance:*** οδηγίες συμμόρφωσης με νόμους όπως ο GDPR.
- Insider Threats: οδηγίες για τον εντοπισμό εσωτερικών απειλών.
- ***Insider Threats:*** εκπαίδευση σχετικά με τον εντοπισμό τεχνικών κοινωνικής μηχανικής που χρησιμοποιούνται για να οδηγήσουν τους χρήστες σε παράνομες ενέργειες που θα έχουν αρνητικό αντίκτυπο στην ασφάλεια ενός οργανισμού.
- ***Browser Security:*** εκπαίδευση σχετικά με τον εντοπισμό ύποπτων ιστότοπων, καθώς και τη σημασία της ενημέρωσης του προγράμματος περιήγησής τους.
- ***Mobile Security***: οδηγίες για την ασφάλεια των κινητών τηλεφώνων.

5.3 Change Management

Η πολιτική διαχείρισης αλλαγών διασφαλίζει ότι οι αλλαγές σε ένα πληροφοριακό σύστημα διαχειρίζονται κεντρικά, γίνονται αποδεκτές και καταγράφονται. Οι αλλαγές πρέπει να γίνονται με τρόπο που να ελαχιστοποιεί τις αρνητικές επιπτώσεις στην παροχή υπηρεσιών. Μια πολιτική διαχείρισης αλλαγών περιλαμβάνει αλλαγές στην ανάπτυξη καθώς και στη συντήρηση λογισμικού, υλικού, βάσεων δεδομένων και διαφόρων άλλων συστημάτων (Mimecast, 2023). Μια πιθανή πολιτική διαχείρισης αλλαγών βασίζεται σε τέσσερα στάδια:

1. ***Κατανόηση της αλλαγής***

Για να προωθήσει κανείς με επιτυχία μια αλλαγή, πρέπει να την κατανοήσει πλήρως. Αυτό περιλαμβάνει την ερώτηση γιατί η αλλαγή είναι απαραίτητη, ποιες θετικές συνέπειες θα έχει για τον οργανισμό, πώς θα επηρεάσει θετικά το προσωπικό, πώς θα επηρεάσει τις εργασιακές διαδικασίες και τι πρέπει να κάνουν οι εργαζόμενοι για να επιτύχουν την αλλαγή. Επιπρόσθετα, πρέπει να ληφθούν υπόψη οι αρνητικές συνέπειες που θα προκύψουν εάν δεν γίνει η αλλαγή. Για να γίνει αποδεκτή μια αλλαγή, πρέπει να υπάρχει ένας βαθμός δυσαρέσκειας με την τρέχουσα κατάσταση. Πρέπει να διασφαλιστεί ότι η αλλαγή θα επιφέρει βελτιωμένες συνθήκες με βεβαιότητα (MindTools, 2023).

2. ***Σχεδιασμός της αλλαγής***

Η αποτελεσματική αλλαγή δεν γίνεται τυχαία. Για να είναι επιτυχής, πρέπει να υπάρχει ένα σχέδιο που να ταιριάζει στον συγκεκριμένο οργανισμό που επιδιώκει την αλλαγή. Κάθε οργανισμός έχει τον δικό του τρόπο να σχεδιάζει αλλαγές, με κάποιους να ακολουθούν αυστηρές μεθοδολογίες και άλλους να είναι πιο ευέλικτοι. Ωστόσο, υπάρχουν ορισμένα γενικά πράγματα που πρέπει να λάβουν υπόψη όλοι. Πρώτον, πρέπει κανείς να εξασφαλίσει υποστήριξη για την αλλαγή, υποστήριξη από τη διοίκηση, τους πόρους και το προσωπικό, καθώς και τον τρόπο με τον οποίο θα χρησιμοποιηθεί αυτή η υποστήριξη. Στη συνέχεια, θα πρέπει κανείς να εξετάσει ποια άτομα μπορούν να βοηθήσουν καλύτερα στο σχεδιασμό και την εφαρμογή της αλλαγής. Η αλλαγή μπορεί να υλοποιηθεί με εσωτερικούς πόρους ή μπορεί να απαιτήσει εξωτερικούς ειδικούς εκτός του οργανισμού. Στη συνέχεια, θα πρέπει να σκεφτεί κανείς πώς η ιδέα της αλλαγής θα αποκτήσει θετική αποδοχή εντός του

οργανισμού. Τέλος, πρέπει να υπάρχει ένα όραμα σχετικά με τον αντίκτυπο της αλλαγής στον οργανισμό (MindTools, 2023).

3. Εφαρμογή Αλλαγής

Το επόμενο στάδιο περιλαμβάνει την εφαρμογή της αλλαγής. Υπάρχουν πολλοί διαφορετικοί τρόποι με τους οποίους μπορεί κανείς να εφαρμόσει αυτή τη διαδικασία. Για παράδειγμα, μπορεί κανείς να ορίσει έναν βαθμό αναγκαιότητας στις ενέργειές τους προκειμένου να οικοδομήσει δυναμική, η οποία θα ενθαρρύνει το υπόλοιπο προσωπικό να υποστηρίξει την αλλαγή. Όποια μέθοδο κι αν επιλέξει κάποιος, εξακολουθούν να υπάρχουν κάποιες γενικές αρχές που πρέπει να ακολουθούνται. Αρχικά, πρέπει να διασφαλιστεί ότι όσοι εμπλέκονται σε αυτή τη διαδικασία κατανοούν τι πρέπει να γίνει, καθώς και τις συνέπειες των αλλαγών. Επιπλέον, πρέπει να καθοριστούν ορισμένοι δείκτες επιτυχίας, οι οποίοι θα παρακολουθούνται συνεχώς για τον έλεγχο της προόδου της διαδικασίας. Θα πρέπει επίσης να παρέχεται οποιαδήποτε απαραίτητη εκπαίδευση για την αλλαγή. Επιπλέον, πρέπει να βρεθούν τρόποι για να αλλάξουν οι συνήθειες των χρηστών και η αλλαγή πρέπει να ενσωματωθεί στην καθημερινή ρουτίνα των χρηστών. Τέλος, πρέπει να παρέχεται υποστήριξη σε όλους καθ' όλη τη διάρκεια της διαδικασίας (MindTools, 2023).

4. Επικοινωνία

Η επικοινωνία είναι το πιο κρίσιμο στοιχείο στη διαχείριση της αλλαγής. Η αλλαγή πρέπει να είναι σαφής και σχετική με τις ανάγκες του οργανισμού, έτσι ώστε οι εργαζόμενοι να μπορούν να κατανοήσουν τι πρέπει να γίνει και γιατί. Επιπλέον, θα πρέπει να τεθεί ο σωστός τόνος για να δημιουργηθεί μια κατάλληλη συναισθηματική απόκριση. Η σύνδεση μιας αλλαγής με τις ανάγκες, την αποστολή ή το όραμα ενός οργανισμού μπορεί να βοηθήσει το προσωπικό να δει πώς η αλλαγή επηρεάζει θετικά τη «μεγάλη εικόνα». Επιπλέον, η καλή διαχείριση της επικοινωνίας και η παροχή της απαραίτητης υποστήριξης σε όσους επιβλέπουν την αλλαγή είναι απαραίτητη. Γενικά, πέντε είναι τα πράγματα που πρέπει να εξασφαλίσει κανείς στον τομέα της επικοινωνίας. Αρχικά, οι ενδιαφερόμενοι πρέπει να γνωρίζουν την ανάγκη για αλλαγή. Στη συνέχεια, θα πρέπει να ενθαρρύνονται να συμμετέχουν και να το υποστηρίζουν. Επιπλέον, θα πρέπει να είναι βέβαιοι ότι η αλλαγή θα γίνει σωστά και ότι έχουν τη δυνατότητα να την πραγματοποιήσουν. Τέλος, είναι απαραίτητο

να παρασχεθεί ψυχολογική ενίσχυση για να διατηρηθεί η απαραίτητη ορμή της διαδικασίας για μεγάλο χρονικό διάστημα (MindTools, 2023).

5.3 Incident Response Policy

Μια πολιτική απόκρισης δείχνει ότι ένας οργανισμός έχει τις απαραίτητες δυνατότητες για να ανιχνεύσει πιθανές επιθέσεις, να επεξεργαστεί το συμβάν και να το επιλύσει. Περιγράφει την ανταπόκριση του οργανισμού σε περίπτωση συμβάντος ασφαλείας, εστιάζοντας σε διαδικασίες που ακολουθούν αμέσως ένα πρόβλημα κυβερνοασφάλειας. Η πολιτική θα πρέπει να περιλαμβάνει πληροφορίες σχετικά με την ομάδα απόκρισης, το προσωπικό που είναι υπεύθυνο για τη δοκιμή της πολιτικής, τον ρόλο κάθε μέλους της ομάδας και τους πόρους που θα χρησιμοποιηθούν για τον εντοπισμό και την ανάκτηση παραβιασμένων δεδομένων (Adsero Security, 2023).

Η συγκεκριμένη πολιτική χωρίζεται σε έξι φάσεις:

1. ***Preparation***

Η φάση προετοιμασίας περιλαμβάνει διαδικασίες που επιτρέπουν σε έναν οργανισμό να ανταποκριθεί αποτελεσματικά σε ένα περιστατικό. Αυτό περιλαμβάνει επίσης τη δημιουργία και την αξιολόγηση πολιτικών, οδηγιών για τον τρόπο απόκρισης, καθώς και των τεχνολογικών εργαλείων που θα χρησιμοποιηθούν. Θα πρέπει να διασφαλίζεται ότι όλα τα τμήματα ενός οργανισμού έχουν εφαρμόσει τις απαραίτητες διαδικασίες για τον περιορισμό και τη διερεύνηση ενός περιστατικού. Εξίσου σημαντική σε αυτή τη φάση είναι η εκπαίδευση του προσωπικού σχετικά με τους ρόλους του στην ομάδα ανταπόκρισης, καθώς και τις ευθύνες που έχουν σε περίπτωση περιστατικού. Θα ήταν ωφέλιμο να διεξάγονται συχνές ασκήσεις προσομοίωσης περιστατικών για την αξιολόγηση του επιπέδου απόκρισης και ετοιμότητας του οργανισμού (Cerrigione, 2015· SecurityMetric, 2023).

2. ***Identification***

Κατά τη φάση της αναγνώρισης αναζητείται η πηγή του συμβάντος. Μπορεί να προκύψει από μια ευπάθεια συστήματος που εκμεταλλεύεται μια εξωτερική ή εσωτερική οντότητα ή από ανθρώπινο λάθος. Όταν εντοπίζεται ένα περιστατικό, η ομάδα απόκρισης θα πρέπει να συλλέγει πληροφορίες, να αποφασίζει για το είδος και τη σοβαρότητα του συμβάντος και να

τεκμηριώνει όλα όσα έγιναν. Η τεκμηρίωση θα πρέπει να απαντά στις ερωτήσεις "πώς, γιατί και πού συνέβη το περιστατικό", πληροφορίες που μπορεί αργότερα να χρειαστούν για νομικούς σκοπούς (Cassetto, 2023 • Adsero Security, 2023).

3. Containment

Σε περίπτωση συμβάντος, η ομάδα απόκρισης πρέπει να το περιορίσει αμέσως για να αποφευχθεί περαιτέρω εξάπλωση. Δεν συνιστάται η διαγραφή ή η καταστροφή οποιουδήποτε λογισμικού ή συστημάτων που εμπλέκονται, καθώς θα εμπόδιζε τη συλλογή δεδομένων. Ο περιορισμός έχει δύο μορφές, βραχυπρόθεσμη και μακροπρόθεσμη. Σε βραχυπρόθεσμο περιορισμό, γίνονται απλές ενέργειες όπως η απομόνωση του τμήματος του δικτύου που δέχεται επίθεση. Σε μακροπρόθεσμο περιορισμό, εκτελούνται ορισμένες βραχυπρόθεσμες ενέργειες, όπως η εφαρμογή προσωρινών επιδιορθώσεων σε ένα παραβιασμένο σύστημα, ενώ ταυτόχρονα δημιουργείται ένα νέο καθαρό σύστημα (Cassetto, 2023 • Adsero Security, 2023).

4. Eradication

Αφού περιοριστεί το πρόβλημα, πρέπει να εντοπιστεί και να εξαλειφθεί η βασική αιτία. Αυτό σημαίνει ότι κάθε είδος κακόβουλου λογισμικού πρέπει να καταστραφεί με ασφάλεια. Τα συστήματα θα πρέπει να ενισχυθούν με μέτρα ασφαλείας και πρέπει να εκτελούνται οι απαραίτητες ενημερώσεις ασφαλείας στο λογισμικό. Η διαδικασία εξάλειψης πρέπει να είναι ολοκληρωμένη. Εάν παραμείνει οποιοδήποτε μέρος του κακόβουλου λογισμικού, θα μπορούσε ενδεχομένως να προκαλέσει άλλο πρόβλημα στο μέλλον (Cassetto, 2023; Adsero Security, 2023).

5. Recovery

Σε αυτό το στάδιο, τα συστήματα που ενεπλάκησαν στο συμβάν επανέρχονται σε ενεργή κατάσταση. Θα πρέπει να δοθεί ιδιαίτερη προσοχή στην απόφαση πότε θα αποκατασταθούν τα συστήματα, πώς θα δοκιμαστεί η κατάσταση των συστημάτων και για πόσο καιρό θα πρέπει να παρακολουθούνται για να διασφαλιστεί η ομαλή λειτουργία τους (Cassetto, 2023; Adsero Security, 2023).

6. Post-Incident

Στο τελικό στάδιο, το περιστατικό θα πρέπει να τεκμηριωθεί πλήρως. Επιπλέον, εάν είναι απαραίτητο, το περιστατικό θα πρέπει να διερευνηθεί περαιτέρω για να κατανοηθεί πλήρως το εύρος του. Τέλος, ολόκληρη η διαδικασία και η πολιτική ασφαλείας θα πρέπει να μελετηθούν, να αξιολογηθούν και να γίνουν οι απαραίτητες βελτιώσεις εάν χρειάζεται (Cassetto, 2023 • Adsero Security, 2023).

5.4 Remote Access Policy

Η πολιτική απομακρυσμένης πρόσβασης παρέχει οδηγίες σχετικά με τον τρόπο ασφαλούς σύνδεσης στο δίκτυο ενός οργανισμού από απομακρυσμένες τοποθεσίες. Με τη σημαντική αύξηση της τηλεργασίας λόγω της πανδημίας COVID-19, αυτή η πολιτική έχει γίνει μια ιδιαίτερα σημαντική πτυχή για την ασφάλεια ενός οργανισμού.

Μια πολιτική απομακρυσμένης πρόσβασης χρησιμεύει ως οδηγός για τον τρόπο με τον οποίο οι χρήστες μπορούν να συνδεθούν με ασφάλεια εξ αποστάσεως και διασφαλίζει ότι η πρόσβαση παρέχεται μόνο σε όσους την χρειάζονται πραγματικά και μόνο εάν οι συσκευές τους πληρούν τις απαραίτητες απαιτήσεις ασφαλείας. Αυτή η πολιτική είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας του δικτύου δεδομένης της αβεβαιότητας που σχετίζεται με την απομακρυσμένη πρόσβαση. Οι άγνωστοι χρήστες που συνδέονται από άγνωστες συσκευές και δίκτυα μπορεί να αποτελέσουν σημαντικό κίνδυνο για έναν οργανισμό, ειδικά αν ληφθεί υπόψη η έλλειψη τεχνικών γνώσεων στην πλειονότητα των χρηστών. Αυτό μπορεί εύκολα να οδηγήσει σε κενά ασφαλείας που μπορούν να εκμεταλλευτούν κακόβουλες οντότητες.

Τέλος, η πολιτική θα πρέπει να ορίζει ποιος είναι υπεύθυνος για τη χορήγηση δικαιωμάτων απομακρυσμένης πρόσβασης στους χρήστες και ποιες ενέργειες μπορούν να εκτελεστούν εξ αποστάσεως. (Carklin, 2021 • RiskOptics, 2022).

5.5 Vendor Management Policy

Ο στόχος της πολιτικής διαχείρισης προμηθευτών/προμηθευτών είναι να εντοπίσει τους συνεργάτες που αποτελούν κίνδυνο για τον οργανισμό και να καθορίσει ενέργειες για την ελαχιστοποίηση του κινδύνου πιθανών επιθέσεων. Αυτή η πολιτική είναι ιδιαίτερα σημαντική στη σημερινή εποχή όπου οι επιθέσεις στην εφοδιαστική αλυσίδα γίνονται όλο και πιο συχνές. Ο πιο συνηθισμένος κίνδυνος δημιουργείται όταν οι προμηθευτές έχουν πρόσβαση σε ευαίσθητα δεδομένα. Οποιοσδήποτε οργανισμός θα πρέπει να είναι σε επαγρύπνηση όταν οι συνεργάτες έχουν πρόσβαση στο δίκτυο του οργανισμού. Περισσότεροι συνεργάτες σημαίνουν περισσότερους στόχους για έναν κυβερνοεγκληματία. Αυτό είναι ιδιαίτερα σημαντικό σε περιπτώσεις εξωτερικής ανάθεσης, μια πρακτική που γίνεται ολοένα και πιο κοινή καθώς επιτρέπει τη μείωση του κόστους ή την εκμετάλλευση της τεχνικής τεχνογνωσίας ενός συνεργάτη.

Η αξιολόγηση των πολιτικών ασφαλείας θα πρέπει να διαδραματίσει σημαντικό ρόλο στην επιλογή ενός συνεργάτη. Η αξιολόγηση αυτών των πολιτικών θα πρέπει πάντα να διενεργείται πριν από την οριστικοποίηση της επιλογής. Όσον αφορά την ασφάλεια στον κυβερνοχώρο, είναι απαραίτητη η συνεχής παρακολούθηση των συνεργατών, καθώς οι αλλαγές στον συνεργαζόμενο οργανισμό μπορούν να δημιουργήσουν κενά ασφαλείας.

Εκτός από τις επιθέσεις στον κυβερνοχώρο, ένας οργανισμός θα πρέπει επίσης να εξετάζει περιπτώσεις όπου ένα στοιχείο μιας διασυνδεδεμένης υπηρεσίας μπορεί να καταστραφεί. Σε αυτές τις περιπτώσεις, είναι σημαντικό να έχετε ένα σχέδιο έκτακτης ανάγκης. Αρχικά θα πρέπει να γνωρίζει κανείς τι επηρεάζεται σε περίπτωση βλάβης στην υπηρεσία συνεργάτη. Τα σημεία αλληλεπίδρασης του συστήματος θα πρέπει να καταγράφονται μαζί με τα στοιχεία επικοινωνίας κάθε συνεργάτη για να διευκολυνθεί η επικοινωνία μεταξύ των αρμόδιων τμημάτων σχετικά με την εξέλιξη του συμβάντος. Στη συνέχεια, θα πρέπει να υπάρχουν εναλλακτικοί τρόποι εκτέλεσης μιας διαδικασίας για να διασφαλιστεί ότι οι λειτουργίες δεν διακόπτονται. Τέλος, θα πρέπει να υπάρχει ένα παραμετροποιημένο σχέδιο απόκρισης για κάθε συνεργάτη ξεχωριστά. Αυτό εξασφαλίζει πιο αποτελεσματική απόκριση σε περίπτωση ζημιάς. Η συνεργασία μεταξύ των ομάδων ασφαλείας των οργανισμών μπορεί να βοηθήσει στην καλύτερη επίλυση προβλημάτων. Ένας τρόπος συνεργασίας είναι η

διεξαγωγή ασκήσεων που προσομοιώνουν πιθανές επιθέσεις (Johnson, 2022; Tunggal, 2023).

5.6 Password Creation and Management Policy

Η παρούσα πολιτική παρέχει οδηγίες για την αποτελεσματική και ασφαλή διαχείριση των κωδικών πρόσβασης για τους χρήστες ενός οργανισμού. Περιλαμβάνει κανόνες για τη δημιουργία κωδικών πρόσβασης, τη χρήση, την αποθήκευση και την αλλαγή τους, καθώς και ένα σχέδιο για την απόκριση σε παραβιάσεις κωδικών πρόσβασης. Δεν πρέπει ποτέ να επιτρέπονται απλοί ή κενοί κωδικοί πρόσβασης. Οι κωδικοί πρόσβασης δεν πρέπει ποτέ να περιέχουν λέξεις που μπορούν να βρεθούν σε ένα λεξικό. Τέτοιοι κωδικοί πρόσβασης είναι ιδιαίτερα ευάλωτοι σε επιθέσεις λεξικών.

Οι κωδικοί πρόσβασης πρέπει να πληρούν ένα ορισμένο επίπεδο πολυπλοκότητας. Θα πρέπει να περιέχουν τουλάχιστον 8 χαρακτήρες, ένα συνδυασμό πεζών και κεφαλαίων χαρακτήρων, καθώς και συγκεκριμένους ειδικούς χαρακτήρες. Οι κωδικοί πρόσβασης δεν πρέπει να περιέχουν προσωπικά δεδομένα όπως αριθμούς φορολογικού μητρώου, αριθμούς κοινωνικής ασφάλισης κ.λπ., καθώς αυτό μπορεί να οδηγήσει σε κλοπή ταυτότητας σε περίπτωση κλοπής του κωδικού πρόσβασης ασφαλείας. Επίσης, προσωπικές πληροφορίες, όπως ονόματα παιδιών, χόμπι, γενέθλια κ.λπ., δεν πρέπει ποτέ να χρησιμοποιούνται, καθώς μπορούν να ληφθούν εύκολα μέσω τεχνικών κοινωνικής μηχανικής. Διαφορετικοί λογαριασμοί σε διαφορετικά συστήματα θα πρέπει να έχουν τους δικούς τους ξεχωριστούς κωδικούς πρόσβασης. Εάν χρησιμοποιείται ο ίδιος κωδικός πρόσβασης, τότε σε περίπτωση παραβίασης, ο ένας λογαριασμός μπορεί εύκολα να παραβιαστεί μαζί με τον άλλο.

Οι χρήστες δεν πρέπει ποτέ να γράφουν τους κωδικούς πρόσβασής τους σε εύκολα προσβάσιμα μέρη ή να τους στέλνουν μέσω email/υπηρεσίας σημειώσεων. Για αυτή την περίπτωση προτείνονται εφαρμογές διαχείρισης κωδικών πρόσβασης, οι οποίες διαθέτουν την απαραίτητη κρυπτογράφηση για την προστασία πολλών κωδικών πρόσβασης. Τέλος, οι χρήστες θα πρέπει να γνωρίζουν ότι το τμήμα πληροφορικής δεν θα ζητήσει ποτέ τους κωδικούς πρόσβασης για κανένα λόγο. Σε περίπτωση απώλειας, θα αντικατασταθεί με μια

προσωρινή που πρέπει να αλλάξουν οι ίδιοι (Montclair State University, 2023; TechRepublic, 2022).

5.7 Access Authorization, Modification and Identify Access Management

Η τρέχουσα πολιτική στοχεύει στη διαχείριση ψηφιακών ταυτοτήτων περιγράφοντας τα κριτήρια για τη δημιουργία ψηφιακών ταυτοτήτων και λογαριασμών, τον τρόπο επαλήθευσης ταυτοτήτων, τη διαχείριση εξουσιοδοτήσεων και τη διαδικασία για έναν λογαριασμό και την καταστροφή ψηφιακών προνομίων. Η πολιτική διαχείρισης πρόσβασης διασφαλίζει ότι κάθε χρήστης που προσπαθεί να αποκτήσει πρόσβαση στο σύστημα είναι αυτός που ισχυρίζεται ότι είναι και εκχωρεί κατάλληλους πόρους. Η διαχείριση πρόσβασης παρέχει ένα πρόσθετο επίπεδο προστασίας μεταξύ των χρηστών και των συστημάτων ενός οργανισμού, το οποίο είναι ιδιαίτερα σημαντικό δεδομένου ότι η κακή διαχείριση πιστοποιητικού πρόσβασης είναι μια από τις πιο κοινές αιτίες προβλημάτων.

Η πολιτική διαχείρισης πρόσβασης χρησιμοποιεί διάφορες πρακτικές για την επίτευξη του στόχου της, ανάλογα με τις περιστάσεις. Η πρώτη πρακτική είναι η Single Sign-On (SSO), η οποία απαιτεί από τους χρήστες να δημιουργούν ισχυρούς κωδικούς πρόσβασης και να τους αλλάζουν περιοδικά, αλλά τους επιτρέπει να έχουν πρόσβαση σε πολλές υπηρεσίες, συχνά από διαφορετικούς παρόχους, χρησιμοποιώντας το ίδιο όνομα χρήστη και κωδικό πρόσβασης. Η δεύτερη πρακτική είναι ο έλεγχος ταυτότητας πολλαπλών παραγόντων, ο οποίος χρησιμοποιεί πρόσθετες μεθόδους ελέγχου ταυτότητας πέρα από έναν απλό κωδικό πρόσβασης.

Η εκχώρηση προνομίων και πόρων βασίζεται επίσης σε δύο πρακτικές. Το πρώτο είναι το Role-Based Access Control, όπου τα δικαιώματα και οι πόροι εκχωρούνται με βάση καθορισμένους ρόλους. Κάθε ρόλος έχει ένα σύνολο προνομίων που επιτρέπουν στον χρήστη να έχει πρόσβαση σε συγκεκριμένες εφαρμογές και λειτουργίες. Ωστόσο, ο Έλεγχος πρόσβασης βάσει ρόλων βασίζεται αποκλειστικά στον έλεγχο ταυτότητας χρήστη για την παραχώρηση προνομίων. Αυτό αυξάνει τον κίνδυνο ζημιάς σε περίπτωση κλοπής των πιστοποιητικών πρόσβασης ενός χρήστη, καθώς όποιος τα χρησιμοποιεί θα έχει τα ίδια προνόμια με τον χρήστη. Η δεύτερη τεχνική εκχώρησης προνομίων είναι ο Έλεγχος πρόσβασης βάσει χαρακτηριστικών, ο οποίος χρησιμοποιεί ένα μοντέλο πρόσβασης που

αξιολογεί χαρακτηριστικά αντί για ρόλους. Αυτά περιλαμβάνουν τοποθεσία, χρονικό εύρος, ημέρες, επίπεδο εκκαθάρισης ασφαλείας, διεύθυνση IP και ούτω καθεξής. Βάσει των συνθηκών πρόσβασης, το επίπεδο προνομίων ενός χρήστη μπορεί να μειωθεί για να αποτρέψει την πρόσβαση σε σημαντικές πληροφορίες και λειτουργίες. Αυτή η πρακτική έχει προληπτικό χαρακτήρα που ενισχύει την ασφάλεια και μειώνει τον κίνδυνο εξωτερικών και εσωτερικών απειλών (Appsian Security, 2021; Gittlen & Rosencrance, 2021).

5.8 Data Retention Policy

Η πολιτική διατήρησης δεδομένων είναι η πρακτική αποθήκευσης και διαχείρισης δεδομένων για καθορισμένο χρονικό διάστημα. Αυτό είναι απαραίτητο για διάφορους λόγους, όπως η τήρηση ακριβών οικονομικών αρχείων, η συμμόρφωση με τους κανονισμούς του κλάδου και τα ρυθμιστικά πλαίσια, καθώς και η διασφάλιση της πρόσβασης σε περίπτωση νομικού συμβάντος. Για να εκπληρώσει αυτές τις υποχρεώσεις, είναι σημαντικό για έναν οργανισμό να έχει μια πολιτική διατήρησης δεδομένων (Qureshi, 2021).

Μια τέτοια πολιτική ορίζει συνήθως (Qureshi, 2021):

- Ποια δεδομένα πρέπει να διατηρηθούν.
- Σε ποια μορφή θα πρέπει να διατηρούνται τα δεδομένα.
- Εάν τα δεδομένα θα πρέπει να διαγραφούν ή να αρχειοθετηθούν μετά την προκαθορισμένη περίοδο διατήρησης.
- Ποιος έχει την εξουσία να καταστρέψει τα δεδομένα.
- Ποια διαδικασία πρέπει να ακολουθηθεί σε περίπτωση παραβίασης πολιτικής.
- Σε ποιο γεωγραφικό πεδίο μπορεί να είναι διαθέσιμα και αποθηκευμένα τα δεδομένα.

Η προκαθορισμένη περίοδος διατήρησης δεδομένων αναφέρεται στο χρονικό διάστημα που απαιτείται από έναν οργανισμό να διατηρήσει πληροφορίες. Διαφορετικοί τύποι δεδομένων έχουν διαφορετικές περιόδους διατήρησης. Αυτά καθορίζονται συνήθως από νόμους και κανονισμούς που απαιτούν συγκεκριμένες περιόδους διατήρησης δεδομένων. Για παράδειγμα, ο ΓΚΠΔ, μέσω του άρθρου 5, ορίζει ότι τα δεδομένα πρέπει να διατηρούνται σε μορφή που να επιτρέπει την ταυτοποίηση των υποκειμένων των δεδομένων για όχι περισσότερο από όσο είναι απαραίτητο για τους σκοπούς για τους οποίους υποβάλλονται

σε επεξεργασία τα δεδομένα προσωπικού χαρακτήρα. Ωστόσο, το άρθρο 89 του GDPR επιτρέπει στους οργανισμούς να αποθηκεύουν δεδομένα προσωπικού χαρακτήρα εάν αυτά τα δεδομένα υποβάλλονται σε επεξεργασία αποκλειστικά για αρχειακούς σκοπούς για λόγους δημοσίου συμφέροντος, επιστημονικούς ή ιστορικούς ερευνητικούς σκοπούς ή στατιστικούς σκοπούς (General Data Protection Regulation (GDPR), 2021).

Λόγω των πολλών νόμων και κανονισμών που υπάρχουν, του μεγέθους ενός οργανισμού, του τύπου του κλάδου στον οποίο συμμετέχει και του είδους των δεδομένων που επεξεργάζεται, δεν υπάρχει ακριβής προσέγγιση. Ωστόσο, υπάρχουν ορισμένες γενικές πρακτικές για τη δημιουργία μιας καλής πολιτικής διατήρησης δεδομένων (Qureshi, 2021):

- ***Νομική έρευνα***: Κάποιος πρέπει να γνωρίζει τους νόμους και τους κανονισμούς που ισχύουν στον κλάδο τους.
- ***Οργανωτικές ανάγκες***: Οι πολιτικές διαχείρισης πρέπει να σχεδιάζονται με τρόπο που να μην επηρεάζει τις σημαντικές λειτουργίες ενός οργανισμού.
- ***Περιεκτικότητα:*** Για να είναι ολοκληρωμένη, μια πολιτική θα πρέπει να περιλαμβάνει άτομα από όλα τα σχετικά τμήματα στη δημιουργία της.
- ***Απλότητα***: Επειδή αυτή η πολιτική αφορά νομικά ζητήματα, θα πρέπει να γράφεται με απλούς όρους που να είναι κατανοητοί από όλους τους εργαζόμενους.
- ***Διαφάνεια:*** Οι πελάτες πρέπει να γνωρίζουν γιατί θα διατηρηθούν οι πληροφορίες τους, πώς θα αποθηκευτούν και πού θα χρησιμοποιηθούν.
- ***Back-up:*** Παρέχει προστασία σε περίπτωση απώλειας δεδομένων.
- ***Διατήρηση δεδομένων***: Τα δεδομένα δεν πρέπει να διατηρούνται περισσότερο από την προκαθορισμένη διάρκειά τους. Η περίσσεια δεδομένων όχι μόνο μειώνει την απόδοση του συστήματος, αλλά επίσης κάνει τον οργανισμό πιο ευάλωτο σε επιθέσεις.

5.9 Bring Your Own Device (BOYD)

Η συγκεκριμένη πολιτική σχετικά με τον τρόπο με τον οποίο οι εργαζόμενοι πρέπει να χρησιμοποιούν τις προσωπικές τους συσκευές για εργασιακούς σκοπούς έχει αποκτήσει σημαντική σημασία λόγω της πανδημίας COVID-19. Η πολιτική Bring Your Own Device (BYOD) έχει πολλά πλεονεκτήματα για έναν οργανισμό, με κύριο όφελος να είναι το οικονομικό. Ο οργανισμός δεν χρειάζεται να ξοδεύει χρήματα σε ηλεκτρονικές συσκευές εργασίας καθώς οι εργαζόμενοι χρησιμοποιούν τις δικές τους. Ωστόσο, αυτό περιπλέκει την επιλογή του λογισμικού εργασίας, καθώς πρέπει να εγκατασταθεί και να λειτουργεί σε διαφορετικά λειτουργικά συστήματα. Ένα άλλο πλεονέκτημα, ιδιαίτερα στην υβριδική ή εξ αποστάσεως εργασία, είναι ο εξοικονομούμενος χρόνος, καθώς ο εξοπλισμός δεν χρειάζεται να σταλεί στους υπαλλήλους. Παρέχει επίσης μεγάλη ευελιξία ως προς το πού και πότε μπορεί κάποιος να εργαστεί. Ωστόσο, υπάρχουν και μειονεκτήματα, με κυριότερο την απώλεια της ιδιωτικής ζωής των εργαζομένων. Ορισμένες εταιρείες μπορεί να θέλουν να παρακολουθούν περισσότερο το ιστορικό email και προγράμματος περιήγησης όταν ένας υπάλληλος χρησιμοποιεί μια προσωπική συσκευή. Ένα άλλο μειονέκτημα είναι η αυξημένη πολυπλοκότητα της τεχνικής υποστήριξης καθώς κάθε σύστημα μπορεί να είναι διαφορετικό (Botha, 2023).

Μια πολιτική BYOD θα πρέπει να ορίζει τα ακόλουθα (Botha, 2023):

- ***Κοινή πλατφόρμα επικοινωνίας***: Θα πρέπει να οριστεί μια κοινή πλατφόρμα επικοινωνίας μεταξύ όλων των συσκευών.
- ***Ιδιοκτησία δεδομένων***: Δεδομένου ότι έχουμε να κάνουμε με προσωπικές συσκευές, θα πρέπει να καθοριστεί αυστηρά ποια δεδομένα στη συσκευή ανήκουν στον οργανισμό. Επίσης, θα πρέπει να καθοριστούν οι απαραίτητες ενέργειες που πρέπει να γίνουν σε περίπτωση που κάποιο μέλος του BYOD αποχωρήσει από τον οργανισμό.
- ***Αυθεντικοποίηση:*** Θα πρέπει να ακολουθούνται οι απαραίτητες πολιτικές ελέγχου ταυτότητας συσκευής και χρήστη.
- ***Εξοπλισμός:*** Σε περίπτωση που απαιτούνται συσκευές με συγκεκριμένες προδιαγραφές, θα πρέπει να ορίζονται στην πολιτική.

- ***Διαφάνεια:*** Η πολιτική θα πρέπει να είναι σαφής σχετικά με τους κινδύνους ασφαλείας που συνεπάγεται αυτή η κίνηση. Θα πρέπει επίσης να είναι σαφές σε θέματα απορρήτου.
- ***Μεταφορά δεδομένων:*** Η μεταφορά δεδομένων πρέπει να γίνεται με ασφάλεια και μόνο μέσω συσκευών αποδεκτών από τον οργανισμό.

5.10 Encryption and Decryption Policy

Αυτή η πολιτική αφορά τη διαδικασία κρυπτογράφησης των δεδομένων ενός οργανισμού. Καθορίζει τους τρόπους με τους οποίους μπορούν να κρυπτογραφηθούν τα δεδομένα, τα προϊόντα που χρησιμοποιούνται για την κρυπτογράφηση, τους αλγόριθμους και τη διαχείριση των κλειδιών κρυπτογράφησης. Είναι μια αμυντική πολιτική που στοχεύει στην εξασφάλιση της προστασίας σημαντικών πληροφοριών. Υπάρχουν διάφοροι τρόποι με τους οποίους ένα σύστημα μπορεί να κρυπτογραφηθεί (Northwestern University, 2023):

- ***Κρυπτογράφηση δίσκου εκκίνησης***: Αυτός ο τύπος κρυπτογράφησης απαιτεί ένα απαραίτητο κλειδί για την εκκίνηση του λειτουργικού συστήματος, καθιστώντας το αρκετά ασφαλές σε περίπτωση κλοπής.
- ***Κρυπτογράφηση email:*** Χρήσιμο σε περιπτώσεις που απαιτείται μη άμεση απομακρυσμένη επικοινωνία.
- ***Κρυπτογράφηση εξωτερικής συσκευής***: Κρυπτογράφηση αφαιρούμενων μέσων αποθήκευσης για ασφαλή μεταφορά εκτός του οργανισμού.
- ***Folder Encryption:*** Κρυπτογράφηση συγκεκριμένων φακέλων για την προστασία τους.
- ***Πλήρης κρυπτογράφηση δίσκου:*** Πλήρης κρυπτογράφηση ενός σκληρού δίσκου, χρήσιμη όταν δεν είναι εγγυημένη η φυσική ασφάλεια.
- ***Κρυπτογράφηση φορητής συσκευής:*** Κρυπτογράφηση κινητής συσκευής για προστασία ευαίσθητων δεδομένων σε περίπτωση κλοπής.
- ***Κρυπτογράφηση επιπέδου μεταφοράς:*** Κρυπτογράφηση συστημάτων μεταφοράς αρχείων.

Πριν ξεκινήσετε τη διαδικασία κρυπτογράφησης, πρέπει πρώτα να ορίσετε ποια δεδομένα θεωρούνται αρκετά ευαίσθητα ώστε να δικαιολογούν την κρυπτογράφηση. Δεν είναι μια απλή διαδικασία, καθώς απαιτεί πάντα τη συνεργασία των ιδιοκτητών τους αφού γνωρίζουν την αξία τους. Στη συνέχεια θα πρέπει να επιλεγούν τα απαραίτητα προϊόντα για την υπηρεσία. Στη συνέχεια, θα πρέπει να δημιουργηθούν κλειδιά κρυπτογράφησης με βάση τις προδιαγραφές κάθε οργανισμού. Τέλος, υπάρχει το στάδιο της διαχείρισης κλειδιών κρυπτογράφησης. Αυτά τα κλειδιά θα πρέπει να φυλάσσονται σε ασφαλή τοποθεσία και να

είναι προσβάσιμα μόνο από εξουσιοδοτημένο προσωπικό, πάντα μέσω ασφαλούς διαδικασίας ελέγχου ταυτότητας.

ΚΕΦΑΛΑΙΟ 6. ΣΥΜΠΕΡΑΣΜΑΤΑ

Κατά τη διάρκεια αυτής της μελέτης, εξετάσαμε όλες τις απειλές για την ασφάλεια στον κυβερνοχώρο που μπορεί να αντιμετωπίσει ένας οργανισμός. Επίσης, καταγράψαμε όλες τις καταστροφικές συνέπειες που ενδέχεται να επηρεάσουν τη λειτουργία του οργανισμού εάν δεν ληφθούν έγκαιρα τα απαραίτητα μέτρα. Στη συνέχεια, αναλύσαμε λεπτομερώς όλα τα μέτρα που μπορούν να ληφθούν για την προστασία ενός οργανισμού, μιας επιχείρησης ή ακόμα και μεμονωμένων χρηστών, ανάλογα με το είδος της επίθεσης. Τέλος, αναλύσαμε διεξοδικά ορισμένες σημαντικές πολιτικές ασφάλειας στον κυβερνοχώρο που κάθε οργανισμός, επιχείρηση, ακόμη και απλοί χρήστες πρέπει να ακολουθούν για να εργάζονται σε ένα ασφαλές περιβάλλον. Επομένως, συμπεραίνουμε ότι από τεχνική άποψη, δεν είναι ιδιαίτερα δύσκολο να διασφαλιστεί ένα ασφαλές περιβάλλον λειτουργίας για έναν οργανισμό. Η δυσκολία και η αποτελεσματικότητα βρίσκονται στην κατασκευή πολιτικών ασφαλείας, καθώς σχεδόν πάντα απαιτείται η συνεργασία πολλαπλών τμημάτων. Ακόμη πιο δύσκολη είναι η εφαρμογή μιας πολιτικής, καθώς δεν μπορεί να διασφαλιστεί ότι θα ακολουθηθεί αυστηρά από όλο το προσωπικό. Συμπερασματικά, καταδείξαμε ξεκάθαρα τη σημασία της ασφάλειας στον κυβερνοχώρο στον ευρύτερο σύγχρονο ψηφιακό χώρο.

Πιο συγκεκριμένα, κάποια βασικά συμπεράσματα μπορούν να εξαχθούν σχετικά με την ασφάλεια στον κυβερνοχώρο. Πρώτα και κύρια, είναι σαφές ότι η κυβερνοασφάλεια είναι ένα κρίσιμο στοιχείο οποιουδήποτε οργανισμού ή επιχείρησης, καθώς οι πιθανοί κίνδυνοι και οι συνέπειες των επιθέσεων στον κυβερνοχώρο μπορεί να είναι σοβαροί. Ως εκ τούτου, είναι επιτακτική ανάγκη οι οργανισμοί να λάβουν σοβαρά υπόψη την ασφάλεια στον κυβερνοχώρο και να εφαρμόσουν μέτρα για την προστασία τους.

Ένας σημαντικός παράγοντας για την ασφάλεια στον κυβερνοχώρο είναι η κατανόηση των διαφορετικών τύπων απειλών και επιθέσεων που μπορεί να συμβούν. Τα στοιχεία που παρουσιάστηκαν επισημαίνουν διάφορους τύπους επιθέσεων, όπως phishing, κακόβουλο λογισμικό και ransomware, μεταξύ άλλων. Έχοντας επίγνωση αυτών των πιθανών απειλών, οι οργανισμοί μπορούν να λάβουν μέτρα για να μετριάσουν τον κίνδυνο να γίνουν θύμα.

Ένας άλλος βασικός παράγοντας για την ασφάλεια στον κυβερνοχώρο είναι η εφαρμογή μέτρων για την προστασία από επιθέσεις. Τα στοιχεία που παρουσιάστηκαν περιγράφουν

διάφορες στρατηγικές που μπορούν να χρησιμοποιήσουν οι οργανισμοί για να προστατευθούν, όπως τείχη προστασίας, συστήματα ανίχνευσης εισβολών και κρυπτογράφηση. Είναι σημαντικό να σημειωθεί ότι καμία μεμονωμένη στρατηγική δεν είναι αλάνθαστη και οι οργανισμοί θα πρέπει να εφαρμόζουν έναν συνδυασμό μέτρων για να παρέχουν την πιο ολοκληρωμένη δυνατή προστασία.

Επιπλέον, η εργασία υπογραμμίζει τη σημασία της ύπαρξης ισχυρών πολιτικών και διαδικασιών για την ασφάλεια στον κυβερνοχώρο. Αυτό περιλαμβάνει τον εντοπισμό ευαίσθητων δεδομένων, την επιλογή κατάλληλων προϊόντων ασφαλείας, τη δημιουργία κλειδιών κρυπτογράφησης και τη διαχείριση της πρόσβασης σε αυτά τα κλειδιά. Οι οργανισμοί πρέπει επίσης να διαθέτουν αποτελεσματικά προγράμματα εκπαίδευσης και ευαισθητοποίησης για να διασφαλίσουν ότι οι εργαζόμενοι κατανοούν τη σημασία της κυβερνοασφάλειας και τον ρόλο τους στην προστασία του οργανισμού.

Τέλος, ενώ είναι τεχνικά εφικτό να εφαρμοστούν αποτελεσματικά μέτρα κυβερνοασφάλειας, η μεγαλύτερη πρόκληση έγκειται στη δημιουργία και την επιβολή πολιτικών για την ασφάλεια στον κυβερνοχώρο. Η συνεργασία μεταξύ των τμημάτων και των εργαζομένων είναι ζωτικής σημασίας για την εφαρμογή και την τήρηση αυτών των πολιτικών. Χωρίς την κατάλληλη συμμόρφωση, ακόμη και τα καλύτερα μέτρα κυβερνοασφάλειας ενδέχεται να μην είναι αποτελεσματικά.

Συμπερασματικά, η κυβερνοασφάλεια είναι ένα κρίσιμο συστατικό οποιουδήποτε οργανισμού ή επιχείρησης. Είναι σημαντικό να κατανοήσουμε τους διαφορετικούς τύπους απειλών και επιθέσεων που μπορούν να προκύψουν, καθώς και να εφαρμόσουμε αποτελεσματικά μέτρα για την προστασία από αυτές. Οι οργανισμοί πρέπει επίσης να διαθέτουν ισχυρές πολιτικές και διαδικασίες κυβερνοασφάλειας και οι εργαζόμενοι πρέπει να γνωρίζουν τον ρόλο τους στην προστασία του οργανισμού. Ενώ η τεχνική σκοπιμότητα είναι σημαντική, η επιτυχία της κυβερνοασφάλειας εξαρτάται τελικά από τη σωστή συμμόρφωση και την επιβολή των πολιτικών.

Βιβλιογραφικές Αναφορές

1. *Address Resolution Protocol (arp)*. Address resolution protocol (ARP). (2023). Retrieved April 21, 2023, from https://erg.abdn.ac.uk/users/gorry/course/inet-pages/arp.html.
2. Adsero Security. (2023). *10 must have IT security policies for every organization*. Adsero Security. Retrieved May 1, 2023, from https://www.adserosecurity.com/security-learning-center/ten-it-security-policies-every-organization-should-have/.
3. Al-Musib, N. S., Al-Serhani, F. M., Humayun, M., & Jhanjhi, N. Z. (2021). Business email compromise (BEC) attacks. *Materials Today: Proceedings*.
4. Appsian Security. (2021). *What is identity and Access Management (IAM)?* Appsian Security. Retrieved May 1, 2023, from https://appsiansecurity.com/identity-and-access-management/.
5. Arampatzis, A. (2022). *What are SSL stripping attacks?* Venafi. Retrieved April 21, 2023, from https://venafi.com/blog/what-are-ssl-stripping-attacks/.
6. Atumu, M. (2021). *Top eight virtualization security issues and risks*. Liquid Web. Retrieved April 21, 2023, from https://www.liquidweb.com/kb/virtualization-security-issues-and-risks/.
7. Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24-31.
8. Berlove, O. (2019). *Man-in-the-middle (MITM) attacks*. PreVeil. Retrieved April 21, 2023, from https://www.preveil.com/blog/man-in-the-middle-mitm-attacks/#:~:text=How%20MITM%20attacks%20intercept%20traffic,the%20wrong%20return%20address%20listed.
9. Botha, C. (2023). *BYOD policy: A step-by-step guide on how to set it up*. Dialpad. Retrieved May 1, 2023, from https://www.dialpad.com/blog/byod-policy/.
10. Carklin, N. (2021). *What is a remote access policy, and why is it important for your organization?* Parallels Remote Application Server Blog - Application virtualization, mobility and VDI. Retrieved May 1, 2023, from https://www.parallels.com/blogs/ras/remote-access-policy/.

11. Cassetto, O. (2023). *Cybersecurity threats: Types and challenges*. Exabeam. Retrieved April 21, 2023, from https://www.exabeam.com/information-security/cyber-security-threat/.
12. Cassetto, O. (2023). *Incident response plan 101: How to build on*. Exabeam. Retrieved May 1, 2023, from https://www.exabeam.com/incident-response/incident-response-plan/.
13. Cerrigione, C. (2015). *Incident response plan*. IT Security. Retrieved May 1, 2023, from https://security.uconn.edu/incident-response-plan/.
14. CIS. (2019). *Ransomware: Facts, threats, and countermeasures*. CIS. Retrieved April 22, 2023, from https://www.cisecurity.org/insights/blog/ransomware-facts-threats-and-countermeasures.
15. Cloudflare. (2023). *What is a ransom ddos attack? | cloudflare*. Cloudflare. Retrieved April 21, 2023, from https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/.
16. Cloudflare. (2023a). *What is a ransom ddos attack?* . Cloudflare. Retrieved April 21, 2023, from https://www.cloudflare.com/learning/ddos/ransom-ddos-attack/.
17. *Confidentiality*. CSRC Content Editor. (2023). Retrieved April 21, 2023, from https://csrc.nist.gov/glossary/term/confidentiality.
18. Coudflare. (2023). *What is the internet of things (IOT)?* Coudflare. Retrieved April 21, 2023, from https://www.cloudflare.com/learning/ddos/glossary/internet-of-things-iot/.
19. Crowdstrike. (2023). *What is an advanced persistent threat (APT)? - crowdstrike*. Crowdstrike. Retrieved April 21, 2023, from https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/.
20. *Cryptojacking*. Interpol. (2023). Retrieved April 21, 2023, from https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking.
21. Curricula. (2022). *Top security awareness training topics for employees*. Curricula. Retrieved May 1, 2023, from https://www.curricula.com/security-awareness-training-topics.

22. *Cyber threat categories and definitions*. Cisco Umbrella. (2023). Retrieved April 21, 2023, from https://umbrella.cisco.com/trends-threats/cyber-threat-categories-and-definitions.
23. *DDoS attack types & mitigation methods: Imperva*. Learning Center. (2022). Retrieved April 21, 2023, from https://www.imperva.com/learn/ddos/ddos-attacks/.
24. DHS GOV. (2018). *Increasing Threats of Deepfake Identities*. DHS GOV. Retrieved April 21, 2023, from https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf.
25. Echr. (2023). *European Court of Human Rights*. HUDOC. Retrieved April 21, 2023, from https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}.
26. *Endpoint security*. Trellix. (2023). Retrieved April 21, 2023, from https://www.trellix.com/en-us/platform/endpoint-security.html.
27. *Enisa Threat Landscape 2021*. ENISA. (2022). Retrieved April 21, 2023, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.
28. *EU imposes the first ever sanctions against cyber-attacks*. European Counsil. (2020). Retrieved April 21, 2023, from https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.
29. Galiveeti, S., Tawalbeh, L. A., Tawalbeh, M., & El-Latif, A. A. A. (2021). Cybersecurity analysis: Investigating the data integrity and privacy in AWS and Azure cloud platforms. In *Artificial Intelligence and Blockchain for Future Cybersecurity Applications* (pp. 329-360). Cham: Springer International Publishing.
30. GeeksforGeeks. (2022). *Session hijacking*. GeeksforGeeks. Retrieved April 21, 2023, from https://www.geeksforgeeks.org/session-hijacking/.
31. General Data Protection Regulation (GDPR). (2018). *Art. 89 GDPR – safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.* Retrieved May 1, 2023, from https://gdpr-info.eu/art-89-gdpr/.

32. General Data Protection Regulation (GDPR). (2021). *Art. 5 GDPR – principles relating to processing of personal data*. Retrieved May 1, 2023, from https://gdpr-info.eu/art-5-gdpr/.
33. Gittlen, S., & Rosencrance, L. (2021). *What is identity and access management? guide to IAM*. Security. Retrieved May 1, 2023, from https://www.techtarget.com/searchsecurity/definition/identity-access-management-IAM-system.
34. Holroyd, M. (2022). *Deepfake video shows Zelenskyy's false call for Ukraine to surrender*. euronews. Retrieved April 21, 2023, from https://www.euronews.com/my-europe/2022/03/16/deepfake-zelenskyy-surrender-video-is-the-first-intentionally-used-in-ukraine-war.
35. IBM. (2023). *What is virtualization?* IBM. Retrieved April 21, 2023, from https://www.ibm.com/topics/virtualization.
36. *Individuals & Families*. Individuals & families | Cyber.gov.au. (2023). Retrieved April 21, 2023, from https://www.cyber.gov.au/taxonomy/term/5.
37. Information Technology. (2020). *It acceptable use policy*. Information Technology. Retrieved May 1, 2023, from https://www.nicholls.edu/information-tech/policyandprocedure/acceptable-use-policy/.
38. *Infosec guide: Mitigating email threats*. InfoSec Guide: Mitigating Email Threats. (2023). Retrieved April 21, 2023, from https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/infosec-guide-email-threats.
39. Johnson, B. (2022, September 9). *How to define your it vendor management policy*. StrongDM. Retrieved May 1, 2023, from https://www.strongdm.com/blog/it-vendor-management-policy.
40. Kaspersky. (2023). *What is cryptojacking and how does it work?* www.kaspersky.com. Retrieved April 21, 2023, from https://www.kaspersky.com/resource-center/definitions/what-is-cryptojacking.
41. Kaspersky. (2023a). *What is a ddos attack? - ddos meaning*. www.kaspersky.com. Retrieved April 21, 2023, from https://www.kaspersky.com/resource-center/threats/ddos-attacks.

42. Kaspersky. (2023b). *What is a cross-site scripting attack? definition and explanation*. www.kaspersky.com. Retrieved April 21, 2023, from https://www.kaspersky.com/resource-center/definitions/what-is-a-cross-site-scripting-attack.
43. Kaspersky. (2023c). *What is an advanced persistent threat (APT)?* Kaspersky. Retrieved April 21, 2023, from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats.
44. Kirsten, S. (2023). *Cross site scripting (XSS)*. Cross Site Scripting (XSS) | OWASP Foundation. Retrieved April 21, 2023, from https://owasp.org/www-community/attacks/xss/.
45. Klein, E. (2021). *How to defend your business against SQL Injections*. Logz.io. Retrieved May 1, 2023, from https://logz.io/blog/defend-against-sql-injections/.
46. Learning center. (2023). *What is a DDoS attack?* Learning center . Retrieved April 21, 2023, from https://community.cloudflare.com/t/learning-center-what-is-a-ddos-attack/338654.
47. Lehto, M. (2013). The cyberspace threats and cyber security objectives in the cyber security strategies. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *3*(3), 1-18.
48. Li, V. (2019). *Polyglot files: A Hacker's best friend*. Medium. Retrieved April 21, 2023, from https://medium.com/swlh/polyglot-files-a-hackers-best-friend-850bf812dd8a.
49. *Malware: What is malware & how to stay protected from malware attacks*. Palo Alto Networks. (2023). Retrieved April 21, 2023, from https://www.paloaltonetworks.com/cyberpedia/what-is-malware.
50. Mandiant. (2023). *DLL side-loading: A Thorn in the side of the anti-virus industry*. Mandiant. Retrieved April 21, 2023, from https://www.mandiant.com/resources/reports/dll-side-loading-thorn-side-anti-virus-industry.
51. McGavran, W. (2009). Intended consequences: regulating cyber attacks. *Tul. J. Tech. & Intell. Prop.*, *12*, 259.

52. Mimecast. (2023). *What are email security threats?: Email threats*. Mimecast. Retrieved April 21, 2023, from https://www.mimecast.com/content/email-threats/.
53. Mimecast. (2023). *What is Security Awareness Training & Why is it important?* Mimecast. Retrieved May 1, 2023, from https://www.mimecast.com/content/what-is-security-awareness-training/.
54. MindTools. (2023). *The Four Principles of Change Management*. MindTools. Retrieved May 1, 2023, from https://www.mindtools.com/ahpnreq/the-four-principles-of-change-management.
55. MIT Media Lab. (2023). *Project Overview ' detect deepfakes: How to counteract misinformation created by ai*. MIT Media Lab. Retrieved May 1, 2023, from https://www.media.mit.edu/projects/detect-fakes/overview/.
56. Montclair State University. (2023). *Password management policy*. Montclair State University. Retrieved May 1, 2023, from https://www.montclair.edu/policies/all-policies/password-management-policy/#:~:text=At%20least%20one%20(1)%20alphabetic,family%20members%2C%20pets%2C%20etc.
57. NewsWatch. (2020). *VM security in 2020: A guide to developing a virtualization security policy*. NewsWatchTV. Retrieved May 1, 2023, from https://newswatchtv.com/2020/10/16/vm-security-2020-guide-developing-virtualization-security-policy/.
58. Northwestern University. (2023). *It policies, standards, and Guidelines*. Information Technology. Retrieved May 1, 2023, from https://www.it.northwestern.edu/about/policies/index.html.
59. OWASP Cheat Sheet Series. (2023). *SQL injection prevention cheat sheet*. SQL Injection Prevention. Retrieved May 1, 2023, from https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html#least-privilege
60. OWASP Cheat Sheet Series. (2023a). *DOM based XSS Prevention Cheat Sheet*. Retrieved May 1, 2023, from https://cheatsheetseries.owasp.org/cheatsheets/DOM_based_XSS_Prevention_Cheat_Sheet.html.

61. OWASP Cheat Sheet Series. (2023β). *Denial of service cheat sheet*. Denial of Service - . Retrieved May 1, 2023, from https://cheatsheetseries.owasp.org/cheatsheets/Denial_of_Service_Cheat_Sheet.html.
62. OWASP Foundation. (2023). *Owasp internet of things*. OWASP Foundation. Retrieved April 21, 2023, from https://owasp.org/www-project-internet-of-things/#tab=IoT_Attack_Surface_Areas.
63. Papez, N., & Shields, R. (2021). *Ransomware countermeasures - mitigation strategies: Proofpoint US*. Proofpoint. Retrieved April 22, 2023, from https://www.proofpoint.com/us/blog/security-awareness-training/countermeasures-ransomware.
64. Penetration Testing Lab. (2013). *Common virtualization vulnerabilities and how to mitigate risks*. Penetration Testing Lab. Retrieved April 21, 2023, from https://pentestlab.blog/2013/02/25/common-virtualization-vulnerabilities-and-how-to-mitigate-risks/.
65. PortSwigger. (2023). *What is dom-based XSS (cross-site scripting)? tutorial & examples: Web security academy*. PortSwigger. Retrieved April 21, 2023, from https://portswigger.net/web-security/cross-site-scripting/dom-based.
66. Qureshi, A. (2021). *Data retention policy 101: Best practices, examples & more*. Intradyn. Retrieved May 1, 2023, from https://www.intradyn.com/data-retention-policy/.
67. *Ransomware:*. The No More Ransom Project. (2023). Retrieved April 21, 2023, from https://www.nomoreransom.org/en/ransomware-qa.html#solution.
68. RiskOptics. (2022). *Why are remote access policies important?* . RiskOptics. Retrieved May 1, 2023, from https://reciprocity.com/resources/why-are-remote-access-policies-important/.
69. SecurityMetrics. (2023). *6 phases in The incident response plan*. SecurityMetrics. Retrieved May 1, 2023, from https://www.securitymetrics.com/blog/6-phases-incident-response-plan.

70. SecurityScorecard. (2023). *How to design an effective cybersecurity policy* Retrieved May 1, 2023, from https://securityscorecard.com/blog/cybersecurity-policy-examples/.
71. Snyder, J. (2022). *3 ways you can mitigate man-in-the-middle attacks*. Samsung Business Insights. Retrieved May 1, 2023, from https://insights.samsung.com/2022/11/23/3-ways-you-can-mitigate-man-in-the-middle-attacks-4/.
72. Souppaya, M., & Scarfone, K. (2013). Guide to malware incident prevention and handling for desktops and laptops. *NIST Special Publication*, *800*, 83.
73. Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45-56.
74. TechRepublic. (2022). *Password management policy*. TechRepublic. Retrieved May 1, 2023, from https://www.techrepublic.com/resource-library/downloads/password-management-policy/.
75. Thakur, K., Qiu, M., Gai, K. and Ali, M.L., 2015, November. An investigation on cyber security threats and security models. In *2015 IEEE 2nd international conference on cyber security and cloud computing* (pp. 307-311). IEEE.
76. The HTTPS-Only Standard. (2023). *HTTP strict transport security*. The HTTPS-Only Standard. Retrieved May 1, 2023, from https://https.cio.gov/hsts/.
77. *Top 10 common types of cybersecurity attacks: Datto Security Solutions*. Datto Security Solutions. (2023). Retrieved April 21, 2023, from https://www.datto.com/blog/common-types-of-cyber-security-attacks.
78. TrendMicro. (2023). *The IOT attack surface: Threats and security solutions*. TrendMicro. Retrieved April 21, 2023, from https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions.
79. Tunggal, A. T. (2023). *Creating a vendor management policy and why you need one: Upguard*. RSS. Retrieved May 1, 2023, from https://www.upguard.com/blog/vendor-management-policy.

80. *Types of cyber attacks - top network security threats*. SolarWinds. (2023). Retrieved April 21, 2023, from https://www.solarwinds.com/types-network-cyber-security-attacks.
81. University IT. (2021). *Acceptable use policy*. University IT. Retrieved May 1, 2023, from https://tech.rochester.edu/policies/acceptable-use-policy/.
82. Velimirovic, A. (2023). *How to prevent ddos attacks: 7 tried-and-tested methods*. phoenixNAP Blog. Retrieved May 1, 2023, from https://phoenixnap.com/blog/prevent-ddos-attacks.
83. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.
84. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.
85. *What are fileless malware attacks and "Living off the land"? unit 42 explains*. Palo Alto Networks. (2023a). Retrieved April 21, 2023, from https://www.paloaltonetworks.com/cyberpedia/what-are-fileless-malware-attacks.
86. *What is a cyber threat?: Upguard*. RSS. (2023). Retrieved April 21, 2023, from https://www.upguard.com/blog/cyber-threat#toc-3.
87. *What is a supply chain attack? solutions & examples: Keeper*. Keeper® Password Manager & Digital Vault. (2023). Retrieved April 21, 2023, from https://www.keepersecurity.com/threats/supply-chain-attack.html.
88. *What is APT (advanced persistent threat): APT security: Imperva*. Learning Center. (2023b). Retrieved April 21, 2023, from https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/.
89. *What is ARP spoofing: Arp cache poisoning attack explained: Imperva*. Learning Center. (2020α). Retrieved April 21, 2023, from https://www.imperva.com/learn/application-security/arp-spoofing/.
90. *What is fileless malware?* Trellix. (2023). Retrieved April 21, 2023, from https://www.trellix.com/en-us/security-awareness/ransomware/what-is-fileless-malware.html.

91. *What is malware and how cybercriminals use it*. McAfee. (2023). Retrieved April 21, 2023, from https://www.mcafee.com/en-us/antivirus/malware.html.
92. *What is MITM (man in the middle) attack: Imperva*. Learning Center. (2019). Retrieved April 21, 2023, from https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/.
93. *What is ransomware?: How to protect against Ransomware*. Malwarebytes. (2022). Retrieved April 21, 2023, from https://www.malwarebytes.com/ransomware.
94. *What is SQL injection: SQLI attack Example & Prevention Methods: Imperva*. Learning Center. (2023a). Retrieved April 21, 2023, from https://www.imperva.com/learn/application-security/sql-injection-sqli/.
95. *What is SSL/TLS encryption?* F5. (2023). Retrieved April 21, 2023, from https://www.f5.com/glossary/ssl-tls-encryption#:~:text=SSL%2FTLS%20uses%20both%20asymmetric,data%20within%20the%20secured%20session.
96. Williams, J. (2020). *Brie Entel*. What You Need To Know About the SolarWinds Supply-Chain Attack | SANS Institute. Retrieved April 21, 2023, from https://www.sans.org/blog/what-you-need-to-know-about-the-solarwinds-supply-chain-attack/.
97. Zerlang, J. (2017). GDPR: a milestone in convergence for cyber-security and compliance. *Network Security*, *2017*(6), 8-11.
98. Zhuang, R., Bardas, A. G., DeLoach, S. A., & Ou, X. (2015, October). A theory of cyber attacks: A step towards analyzing MTD systems. In *Proceedings of the second ACM workshop on moving target defense* (pp. 11-20).
99. *Ransomware Examples: 16 Recent Ransomware attacks.* (2023). Retrieved Aril 21 , 2023 , from 16 Ransomware Examples From Recent Attacks - CrowdStrike